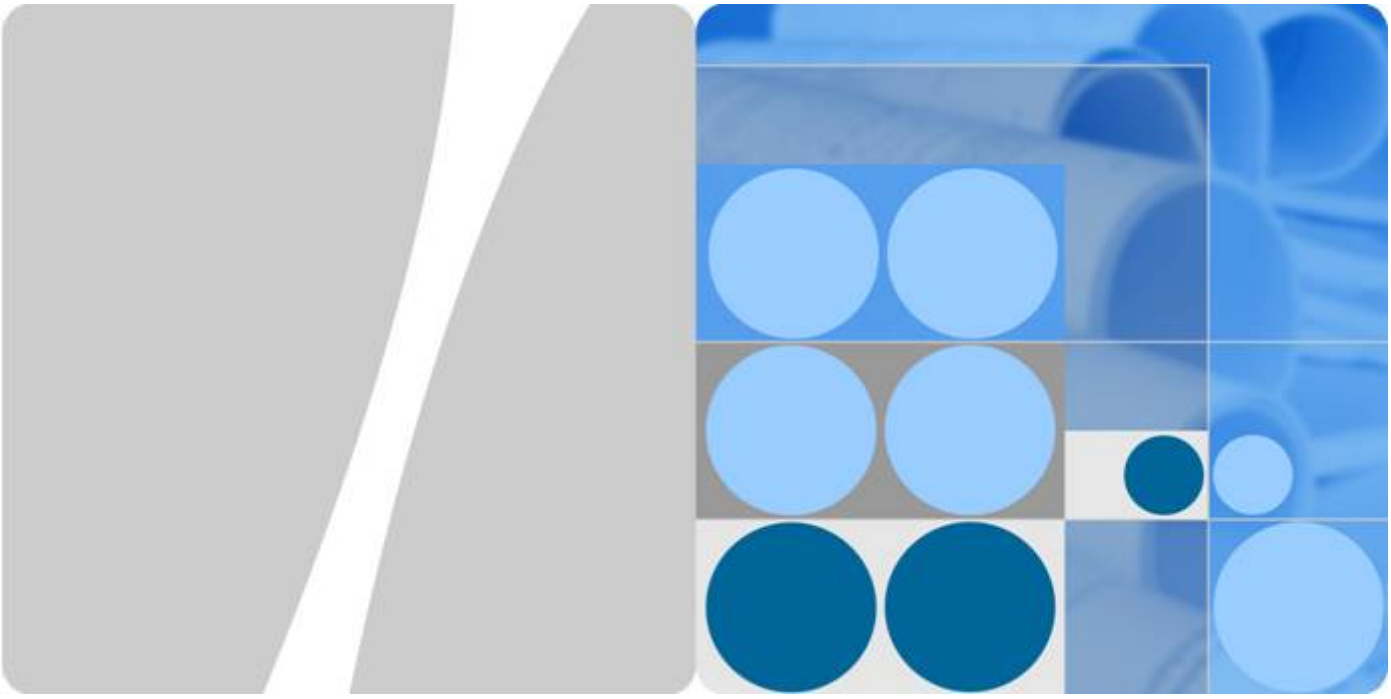


Enterprise Data Communication Products

Feature Description - WLAN

Issue 02

Date 2013-05-15

HUAWEI TECHNOLOGIES CO., LTD.

HUAWEI

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://enterprise.huawei.com

About This Document

Intended Audience

This document describes the definition, purpose, and implementation of features on enterprise datacom products including the campus network switch, enterprise router, data center switch, and WLAN. For features supported by the device, see *Configuration Guide*.

This document is intended for:

- Network planning engineers
- Commissioning engineers
- Data configuration engineers
- System maintenance engineers

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
DANGER	Indicates a hazard with a high level or medium level of risk which, if not avoided, could result in death or serious injury.
WARNING	Indicates a hazard with a low level of risk which, if not avoided, could result in minor or moderate injury.
CAUTION	Indicates a potentially hazardous situation that, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results.
TIP	Provides a tip that may help you solve a problem or save time.
NOTE	Provides additional information to emphasize or supplement important points in the main text.

Command Conventions

The command conventions that may be found in this document are defined as follows.

Convention	Description
Boldface	The keywords of a command line are in **boldface**.
Italic	Command arguments are in *italics*.
[ ]	Items (keywords or arguments) in brackets [ ] are optional.
{ x | y | ... }	Optional items are grouped in braces and separated by vertical bars. One item is selected.
[x | y | ...]	Optional items are grouped in brackets and separated by vertical bars. One item is selected or no item is selected.
{ x | y | ... }*	Optional items are grouped in braces and separated by vertical bars. A minimum of one item or a maximum of all items can be selected.
[x | y | ...]*	Optional items are grouped in brackets and separated by vertical bars. You can select one or several items, or select no item.
&<1-n>	The parameter before the & sign can be repeated 1 to n times.
#	A line starting with the # sign is comments.

Change History

Changes between document issues are cumulative. Therefore, the latest document version contains all updates made to previous versions.

Changes in Issue 02 (2013-05-15)

This version has the following updates:

The following information is modified:

- Descriptions and figures are optimized, improving availability.

Changes in Issue 01 (2012-09-30)

Initial commercial release.

Contents

About This Document.....ii

1 WLAN Basics.....1

1.1 Introduction to WLAN.....2
1.2 Principles.....2
1.2.1 Concepts.....2
1.2.2 802.11 Standards.....4
1.2.3 WLAN Architecture.....9
1.2.4 AP Login.....11
1.2.5 STA Access.....15
1.2.6 Data Forwarding Mode.....18
1.3 Applications.....22
1.3.1 WLAN Networking Application on Medium- and Large-sized Campus Networks.....22
1.3.2 WLAN Networking Application on Small Campus Networks.....24
1.3.3 WLAN Networking Application in Enterprise Branches.....25
1.3.4 SOHO WLAN Networking Application.....26
1.4 References.....26

2 WLAN Security.....28

2.1 Introduction to WLAN Security.....29
2.2 Perimeter Security Principles.....29
2.2.1 Wireless Intrusion Detection.....29
2.2.2 Wireless Intrusion Prevention.....31
2.2.3 Attack Detection.....32
2.2.4 Defense Against Brute Force Attacks on PSK.....34
2.3 User Access Security Principles.....35
2.3.1 Security Policy.....35
2.3.1.1 WEP.....35
2.3.1.2 WPA/WPA2.....35
2.3.1.3 WAPI.....41
2.3.2 STA Blacklist and Whitelist.....46
2.4 Service Security Principles.....47
2.4.1 User Isolation.....47
2.4.2 Terminal Type Identification.....48

2.5 Applications....50
2.5.1 WIDS/WIPS....50
2.5.2 Security Policy....51
2.5.3 STA Blacklist and Whitelist....52
2.6 References....53
3 Radio Resource Management....54
3.1 Introduction to Radio Resource Management....55
3.2 Principles....55
3.2.1 Radio Calibration....55
3.2.2 Load Balancing....60
3.2.3 5G-Prior Access....63
3.2.4 Spectrum Analysis....63
3.3 References....65
4 WLAN Reliability....66
4.1 Introduction to WLAN Reliability....67
4.2 Principles....67
4.2.1 Non-Stop AP Operation After CAPWAP Link Disconnection....67
4.2.2 Dual-Link Backup....69
4.2.3 AC Hot Standby....71
4.3 Applications....73
4.3.1 Application of Non-Stop AP Operation After CAPWAP Link Disconnection....73
4.3.2 Application of Dual-Link Backup....74
4.3.3 Application of AC Hot Standby....75
4.4 References....77
5 WLAN Roaming....78
5.1 Introduction to WLAN Roaming....79
5.2 Principles....80
5.2.1 Roaming Between APs in the Same Service VLAN....80
5.2.2 Roaming Between APs in Different Service VLANs....82
5.2.3 Key Negotiation Between STA and AP....83
5.3 References....84
6 WLAN QoS....85
6.1 Introduction to WLAN QoS....86
6.2 Principles....86
6.2.1 WMM....87
6.2.2 Priority Mapping....91
6.2.3 Traffic Policing....92
6.3 Applications....96
6.4 References....97
7 WLAN WDS....98

7.1 Introduction to WDS....99
7.2 Principles....99
7.3 Applications....103
7.4 References....105
8 WLAN Mesh....106
8.1 Introduction to WLAN Mesh....107
8.2 Principles....107
8.3 Applications....112
8.4 References....114
9 WLAN Positioning....115
9.1 Introduction to Wireless Positioning....116
9.2 Principles....116
9.2.1 WLAN tag positioning....116
9.2.2 Terminal Positioning....119
9.3 References....122

1 WLAN Basics

About This Chapter

1.1 Introduction to WLAN

1.2 Principles

1.3 Applications

1.4 References

1.1 Introduction to WLAN

Definition

A wireless local area network (WLAN) is a network that uses wireless channels such as radio waves, laser, and infrared rays to replace the transmission media used on a wired LAN. The WLAN technology described in this document is implemented based on 802.11 standards. That is, a WLAN is a network that uses high-frequency signals (for example, 2.4 GHz or 5 GHz signals) as transmission media.

802.11 was originally a wireless LAN communications standard defined by the Institute of Electrical and Electronics Engineers (IEEE) in 1997. The IEEE then made amendments to the standard, forming the 802.11 family, including 802.11, 802.11a, 802.11b, 802.11e, 802.11g, 802.11i, and 802.11n.

Purpose

Wired LANs use wired cables or optical fibers as transmission media, which are expensive and have fixed locations. As people have increasing requirements on network mobility, wired LANs cannot meet these requirements. WLAN technology is then developed. Currently, WLAN has become a cost-efficient network access mode. WLAN technology allows you to easily access a wireless network and move around within the coverage of the wireless network.

Benefits

- High network mobility: WLANs can be connected easily, which is not limited by cable and port positions. WLANs especially apply to scenarios such as office buildings, airport halls, resorts, hotels, stadiums, and cafes.
- Flexible network deployment: WLANs can provide wireless network coverage in places where cables are difficult to deploy, such as subways and highways. This solution reduces cables, offers ease of implementation at a low cost, and has high scalability.

1.2 Principles

1.2.1 Concepts

- Station (STA): a terminal that supports 802.11 standards, such as a PC that has a wireless NIC or a mobile phone that supports WLAN.
- Radio signal: high-frequency electromagnetic wave that has long-distance transmission capabilities. Radio signals provide transmission media for 802.11-compliant WLANs. Radio signals described in this document are electromagnetic waves in 2.4 GHz or 5 GHz frequency band.
- Access point (AP): a device that provides 802.11-compliant wireless access for STAs to connect wired networks to wireless networks. APs fall into two categories:
  - Fat AP: provides wireless access for STAs in the **autonomous architecture**. A Fat AP provides wireless connection, security, and management functions.

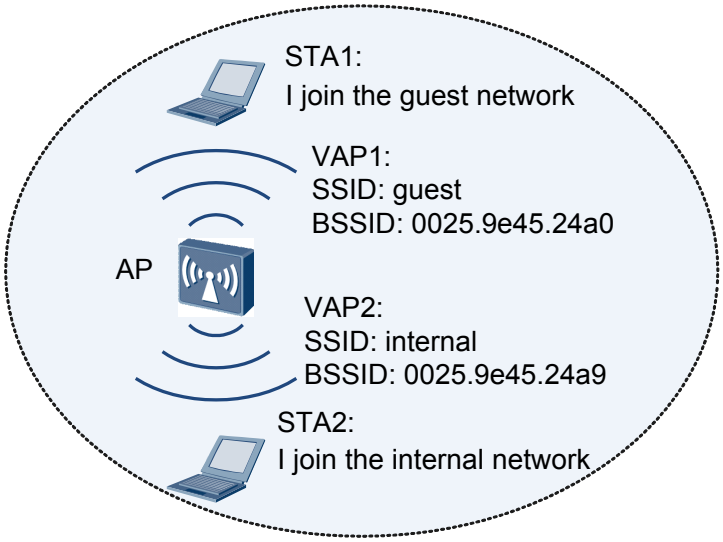
  - Fit AP: provides wireless access for STAs in the **centralized architecture**. A Fit AP provides only reliable, high-performance wireless connection and depends on an access controller (AC) to provide other functions.

- AC: a device that controls and manages all the APs on a WLAN in the centralized architecture. For example, an AC can connect to an authentication server to authenticate WLAN users.
- Control And Provisioning of Wireless Access Points (CAPWAP): an encapsulation and transmission mechanism defined in RFC 5415 to implement communication between APs and ACs.
- Virtual access point (VAP): a WLAN service entity on an AP. You can create different VAPs on an AP to provide wireless access service for different user groups.
- AP region: a collection of APs. AP regions are configured based on AP deployment on enterprise networks. Generally, a region maps a hotspot.
- Service set identifier (SSID): a unique identifier that identifies a wireless network. When you search for available wireless networks on your laptop, SSIDs are displayed to identify the available wireless networks.

  SSIDs are classified into two types:

  - Basic service set identifier (BSSID): a link-layer MAC address of a VAP on an AP. **Figure 1-1** shows the relationship between VAP and BSSID.

    Figure 1-1 Relationship between VAP and BSSID

  - Extended service set identifier (ESSID): an identifier of one or a group of wireless networks. For example, in **Figure 1-1**, SSID **guest** identifies a wireless network, and SSID **internal** identifies another wireless network. A STA scans all wireless networks and selects a wireless network based on the SSID. Generally, an SSID refers to an ESSID.

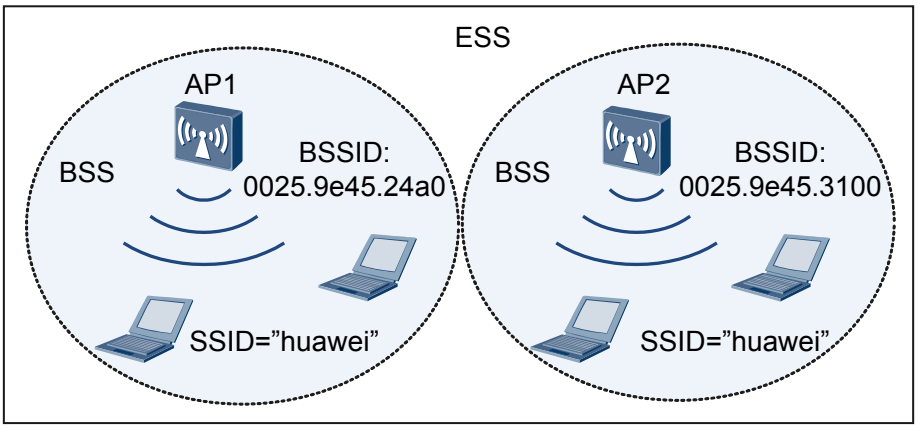
    NOTE

    Multiple APs can use one ESSID to provide roaming service for users; however, their BSSIDs must be unique because the MAC address of each AP is unique.

- Basic service set (BSS): an area covered by an AP. STAs in a BSS can communicate with each other.
- Extend service set (ESS): a group of BSSs that share the same SSID.

Figure 1-2 shows the relationship between SSID, BSSID, BSS, and ESS.

Figure 1-2 Relationship between SSID, BSSID, BSS, and ESS

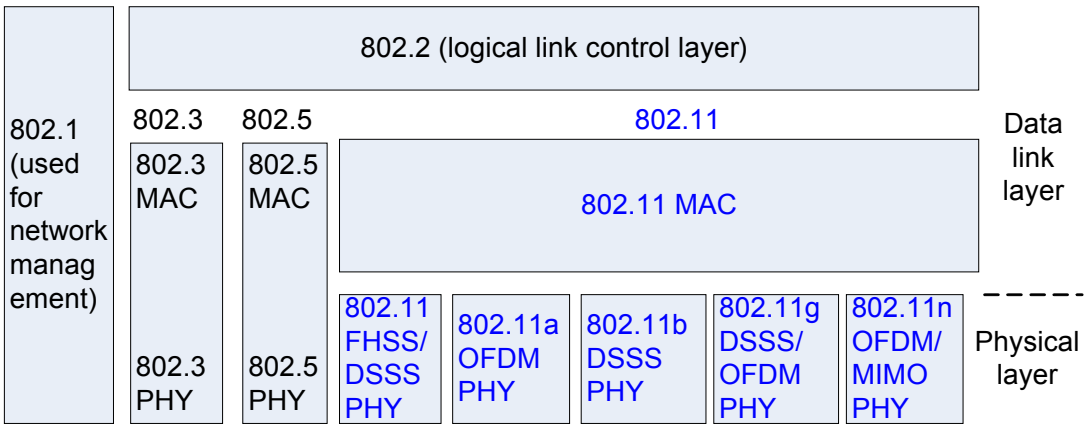


1.2.2 802.11 Standards

Introduction to 802.11

Figure 1-3 shows the role of 802.11 standards in the IEEE 802 standard family, involving the physical layer and data link layer.

Figure 1-3 Role of 802.11 standards in the IEEE 802 standard family



- Physical Layer

  802.11 standards use different physical layer technologies, including frequency hopping spread spectrum (FHSS), direct sequence spread spectrum (DSSS), orthogonal frequency division multiplexing (OFDM), and multiple-input multiple-output (MIMO). These physical layer technologies support different frequency bands and transmission rates, as shown in **Table 1-1**.

Table 1-1 Comparisons between 802.11 standards

802.11 Standard	Physical Layer Technology	Frequency Band (GHz)	Transmission Rate (Mbit/s)	Compatibility with Other 802.11 Standards	Commercial Use
802.11	FHSS/ DSSS	2.4	1, 2	Incompatible	Earlier standard, supported by most products
802.11b	DSSS	2.4	1, 2, 5.5, 11	Incompatible	Earlier standard, supported by most products
802.11a	OFDM	5	6, 9, 12, 18, 24, 36, 48, 54	Incompatible	Rarely used
802.11g	DSSS/ OFDM	2.4	1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, 54	Compatible with 802.11b	Widely used
802.11n	OFDM/ MIMO	2.4, 5	A maximum of 600 Mbit/s, depending on the modulation and coding scheme (MCS)	Compatible with 802.11a, 802.11b, and 802.11g	Widely used

- Data Link Layer

  On a wired LAN, 802.3 standards use the carrier sense multiple access with collision detection (CSMA/CD) mechanism to control wired media access of different devices. The CSMA/CD mechanism requires that all terminals should detect packets of each other. However, WLANs provide only limited wireless signal coverage, so some terminals may fail to detect the packets of each other. 802.11 standards use the carrier sense multiple access with collision avoidance (CSMA/CA) mechanism to overcome the deficiency in the CSMA/CD mechanism.

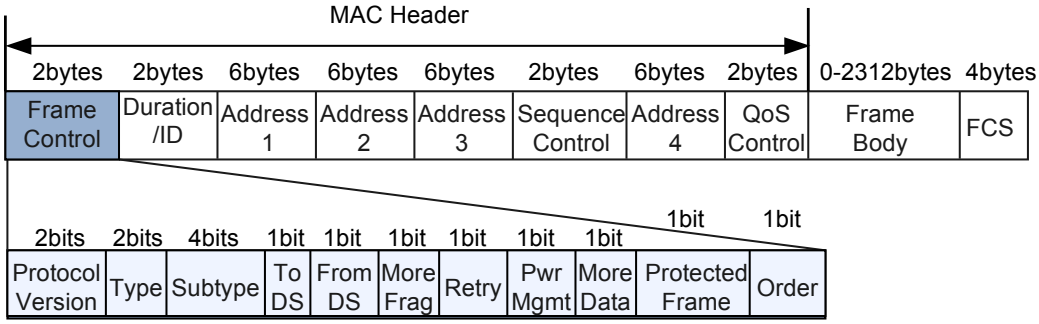
  NOTE

  For CSMA/CA principles, see **6.2.1 WMM**.

802.11 MAC Frame Format

An 802.11 MAC frame consists of a MAC header, frame body, and frame check sequence (FCS). The settings of attribute fields in the MAC header determine the frame type. **Figure 1-4** shows the 802.11 MAC frame format.

Figure 1-4 802.11 MAC frame format



An 802.11 MAC frame has a maximum length of 2348 bytes. The following describes the meanings of each field in an 802.11 MAC frame.

- Frame Control field: includes the following sub-fields:
  - Protocol Version: indicates the MAC version of the frame. Currently, only MAC version 0 is supported.
  - Type/Subtype: identifies the frame type, including data, control, and management frames.
    - Data frame: transmits data packets, including a special type of frame: Null frame. A Null frame has a zero-length frame body. A STA can send a Null frame to notify an AP of the changes in the power-saving state.

      NOTE

      802.11 supports the power-saving mode, allowing STAs to shut down antennas to save power when no data is transmitted.
    - Control frame: helps transmit data frames, releases and obtains channels, and acknowledges received data. Some common control frames include:
      - Acknowledgement (ACK) frame: After receiving a data frame, the receiving STA will send an ACK frame to the sending STA if no error is detected.
      - Request to Send (RTS) and Clear to Send (CTS) frames: provide a mechanism to reduce collisions for APs with hidden STAs. A STA sends an RTS frame before sending data frames. The STA that receives the RTS frame responds with a CTS frame. This mechanism is used to release a channel and enable a sending STA to obtain data transmission media.
    - Management frame: manages WLANs, including notifying network information, adding or removing STAs, and managing radio. Some common management frames include:
      - Beacon frame: is periodically sent by an AP to announce the WLAN presence and provide WLAN parameters (for example, the SSID, supported rate, and authentication type).
      - Association Request/Response frame: A STA sends an Association Request frame to an AP to request to join a WLAN. After receiving the Association

Request frame, the AP sends an Association Response frame to the STA to accept or reject the association request.

- Disassociation frame: is sent from a STA to terminate the association with an AP.
- Authentication Request/Response frame: is used in link authentication between a STA and an AP for identity authentication.
- Deauthentication frame: is sent from a STA to terminate link authentication with an AP.
- Probe Request/Response frame: A STA or an AP sends a Probe Request frame to detect available WLANs. After another STA or AP receives the Probe Request frame, it needs to reply with a Probe Response frame that carries all parameters specified in a Beacon frame.

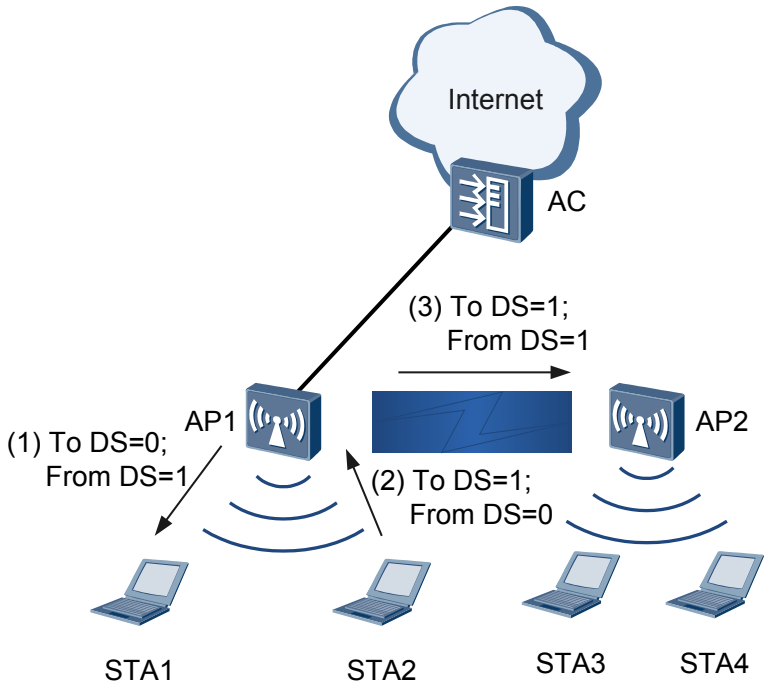
- To DS and From DS: indicate whether a data frame is destined for a distribution system (or an AP). If the two fields are set to 1, the data frame is transmitted between APs.
- More Frag: indicates whether a packet is divided into multiple fragments for transmission.
- Retry: indicates whether a frame needs to be retransmitted. This field helps eliminate duplicate frames.
- Pwr Mgmt: indicates the power management mode of a STA after the completion of a frame exchange, including Active and Sleep modes.
- More Data: indicates that an AP transmits buffered packets to a STA in power-saving mode.
- Protected Frame: indicates whether a frame is encrypted.
- Order: indicates whether a frame is transmitted in order.

- Duration/ID field: has the following forms:
  - Duration: indicates the duration in which a STA can occupy a channel. This field is used for CSMA/CA.
  - Contention-Free Period (CFP): has a value of 32768, indicating that a STA keeps occupying a channel and other STAs cannot use the channel.
  - Association ID (AID): identifies the BSS to which a STA belongs. This field is carried in a PS-Poll frame. A STA may work in active or sleep mode. When a STA works in sleep mode, an AP buffers data frames destined for the STA. When the STA transitions from the sleep mode to the active mode, the STA sends a PS-Poll frame to request the buffered data frames.
- Address field: indicates MAC addresses. An 802.11 frame can have up to four address fields. The four address fields vary according to the To DS/From DS sub-field in the Frame Control field. For example, the values of the four address fields are different when a frame is sent from a STA to an AP and when a frame is sent from an AP to a STA. **Table 1-2** describes the rules for filling in the four address fields.

Table 1-2 Rules for filling in the four address fields

To DS	From DS	Address 1	Address 2	Address 3	Address 4	Description
0	0	Destination address	Source address	BSSID	Unused	The frame is a management or control frame, for example, a Beacon frame sent by an AP.
0	1	Destination address	BSSID	Source address	Unused	AP1 sends the frame to STA1 as shown in (1) in **Figure 1-5**.
1	0	BSSID	Source address	Destination address	Unused	STA2 sends the frame to AP1 as shown in (2) in **Figure 1-5**.
1	1	BSSID of the destination AP	BSSID of the source AP	Destination address	Source address	AP1 sends the frame to AP2 as shown in (3) in **Figure 1-5**.

Figure 1-5 WLAN networking



- Sequence Control field: is used to eliminate duplicate frames and reassemble fragments. It includes two sub-fields:
  - Fragment Number: is used to reassemble fragments.
  - Sequence Number: is used to eliminate duplicate frames. When a device receives an 802.11 MAC frame, the device discards the frame if its Sequence Number field value is the same as a previous frame.
- QoS Control field: exists only in a data frame to implement 802.11e-compliant WLAN QoS.
- Frame Body field: transmits payload from higher layers. It is also called the data field. In 802.11 standards, the transmitted payload is also called a MAC service data unit (MSDU).
- Frame Check Sequence (FCS) field: checks the integrity of received frames. The FCS field is similar to the cyclic redundancy check (CRC) field in an Ethernet packet.

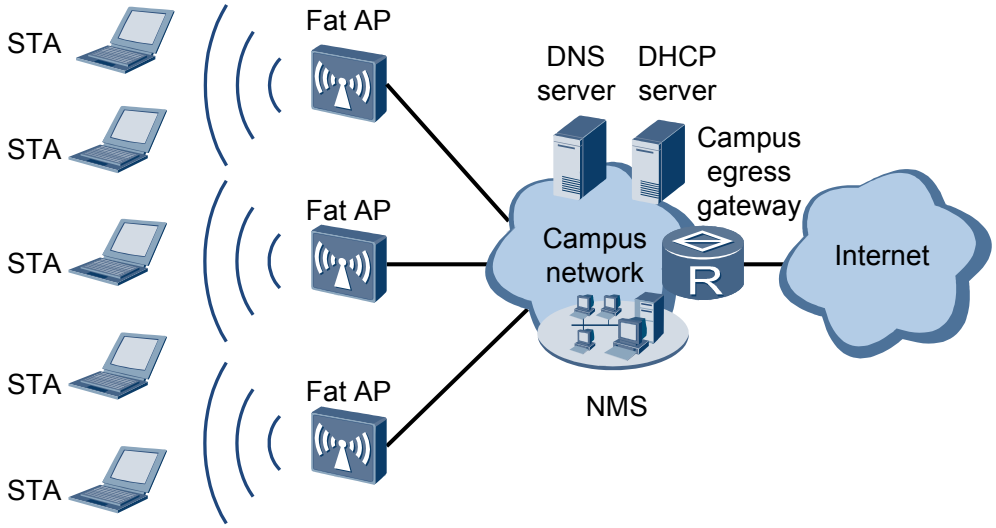
1.2.3 WLAN Architecture

A WLAN has the wired side and wireless side. On the wired side, an AP connects to the Internet using Ethernet. On the wireless side, a STA communicates with an AP using 802.11. The WLAN architecture on the wireless side includes the autonomous architecture and centralized architecture.

Autonomous Architecture

In autonomous architecture, Fat APs implement wireless access without requiring an AC, as shown in **Figure 1-6**.

Figure 1-6 WLAN autonomous architecture

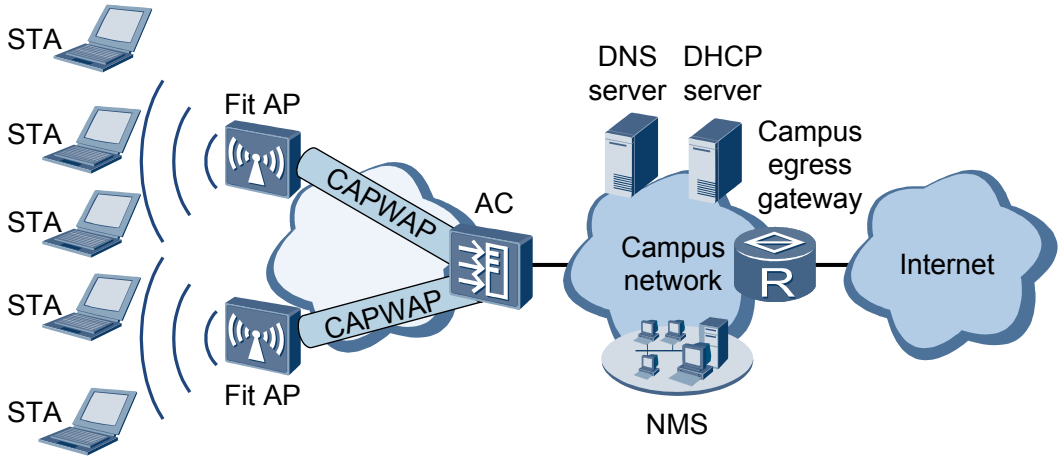


The autonomous architecture was widely used in early stage of WLAN construction. Fat APs have powerful functions and can work independently of ACs; however, Fat APs have complex structure and are difficult to manage in a centralized manner. When an enterprise has a large number of APs deployed, AP configuration and software upgrade bring large workload and high costs. Therefore, the autonomous architecture is gradually replaced by the centralized architecture.

Centralized Architecture

In centralized architecture, an AC manages and controls multiple APs (Fit APs) in centralized manner, as shown in **Figure 1-7**.

Figure 1-7 WLAN centralized architecture



In centralized architecture, APs work with an AC to implement wireless access.

- The AC implements all security, control, and management functions, including mobile user management, identity authentication, VLAN assignment, radio management, and data forwarding.

- Fit APs implement wireless radio access, including radio signal transmission and detection response, data encryption and decryption, and data transmission acknowledgment.
- The AC and APs communicate using Control and Provisioning of Wireless Access Points (CAPWAP). They can be connected across a Layer 2 or Layer 3 network.

The centralized architecture applies to enterprise networks and carrier networks because it allows centralized management and maintenance. The centralized architecture is used in the following sections.

In autonomous architecture, STAs associate with a Fat AP to access a WLAN. For details, see **1.2.5 STA Access**.

In centralized architecture, wireless access involves the following operations:

1. Fit APs establish CAPWAP tunnels with an AC. For details, see **1.2.4 AP Login**.
2. Fit APs associate with an AC. For details, see **1.2.5 STA Access**.

1.2.4 AP Login

In centralized architecture, Fit APs need to go online before being managed and controlled by an AC. AP login includes the following phases:

1. **IP Address Allocation**
2. **CAPWAP Tunnel Establishment**
3. **AP Access Control**
4. **(Optional) AP Software Upgrade**
5. **CAPWAP Tunnel Maintaining**
6. **AC Configuration Delivery**

IP Address Allocation

An AP obtains an IP address in any of the following modes:

- Static mode: An IP address is configured for the AP.
- DHCP mode: The AP functions as a DHCP client to request an IP address from a DHCP server.
- PPPoE mode: The AP functions as a PPPoE client to request an IP address from a PPPoE server.

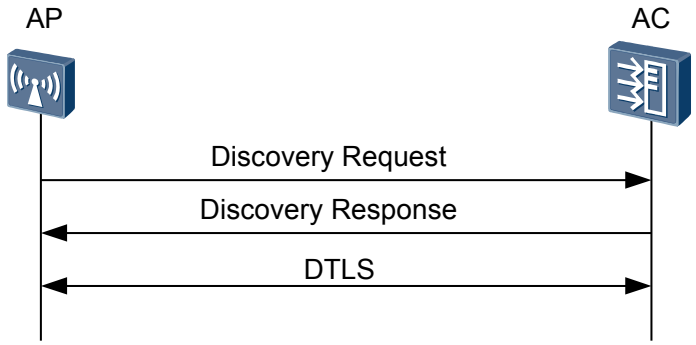
CAPWAP Tunnel Establishment

The AC manages and controls APs in a centralized manner through CAPWAP tunnels. CAPWAP tunnels provide the following functions:

- Maintains the running status of APs and the AC.
- Helps the AC manage APs and deliver configurations to APs.
- Transmits service data to the AC for centralized forwarding.

Figure 1-8 shows the process of establishing a CAPWAP tunnel.

Figure 1-8 CAPWAP tunnel establishment process



1. Discovery phase (an AP discovers an AC): An AP sends a Discovery Request packet to find an available AC.

   An AP can discover an AC in static or dynamic mode.

   - **Static mode**

     An AC IP address list is preconfigured on the AP. When the AP goes online, the AP unicasts a Discovery Request packet to each AC whose IP address is specified in the preconfigured AC IP address list. After receiving the Discovery Request packet, the ACs send Discovery Response packets to the AP. The AP then selects an AC to establish a CAPWAP tunnel according to the received Discovery Request packets.

   - **Dynamic mode**

     An AP can dynamically discover an AC in DHCP, DNS, or broadcast mode.

     - DHCP mode: The AP obtains an AC IP address using DHCP and then unicasts a Discovery Request packet to the AC. After receiving the Discovery Request packet, the AC sends a Discovery Response packet to the AP. The AC IP address is obtained from the AC IP address list contained in Option 43 carried in a DHCP Response packet and configured on a DHCP server.
     - DNS mode: The AP obtains an AC domain name and DNS server IP address using DHCP and then requests to obtain the IP address mapped the AC domain name from the DNS server. After obtaining the AC IP address, the AP unicasts a Discovery Request packet to the AC. The AC then sends a Discovery Response packet to the AP. The AC domain name is carried in Option 15 that is contained in a DHCP Response packet and configured on a DHCP server.

       After receiving the DHCP Response packet, the AP obtains the AC domain name carried in Option 15. The AP then automatically adds the prefix **huawei-wlan-controller** to the obtained domain name and sends it to the DNS server to obtain the IP address corresponding to the AC domain name. For example, after obtaining the AC domain name **ac.test.com** configured on the DHCP server, the AP adds the prefix **huawei-wlan-controller** to **ac.test.com** and sends the **huawei-wlan-controller.ac.test.com** to the DNS server for resolution. The IP address corresponding to **huawei-wlan-controller.ac.test.com** must be configured on the DNS server.
     - Broadcast mode: The AP broadcasts a Discovery Request packet to automatically discover an AC and then selects an AC to establish a CAPWAP tunnel according to the Discovery Response packets received from available ACs when the following conditions are met:

- The AP and ACs reside on the same network segment.
- No AC IP address list is configured on the AP; alternatively, an AC IP address is configured on the AP but the AP does not receive any Discovery Response packet after sending a Discovery Request packet 10 times.
- **Dual-Link Backup** is not configured on the AP.

2. The AP establishes CAPWAP tunnels with an AC.

   CAPWAP tunnels include data tunnels and control tunnels.

   - Data channel: transmits service data from the AP to an AC for centralized forwarding.
   - Control tunnel: transmits control packets between the AP and AC. You can also enable datagram transport layer security (DTLS) encryption over the control tunnel to ensure security of CAPWAP control packets. Subsequently, CAPWAP control packets will be encrypted and decrypted through DTLS.

   NOTE

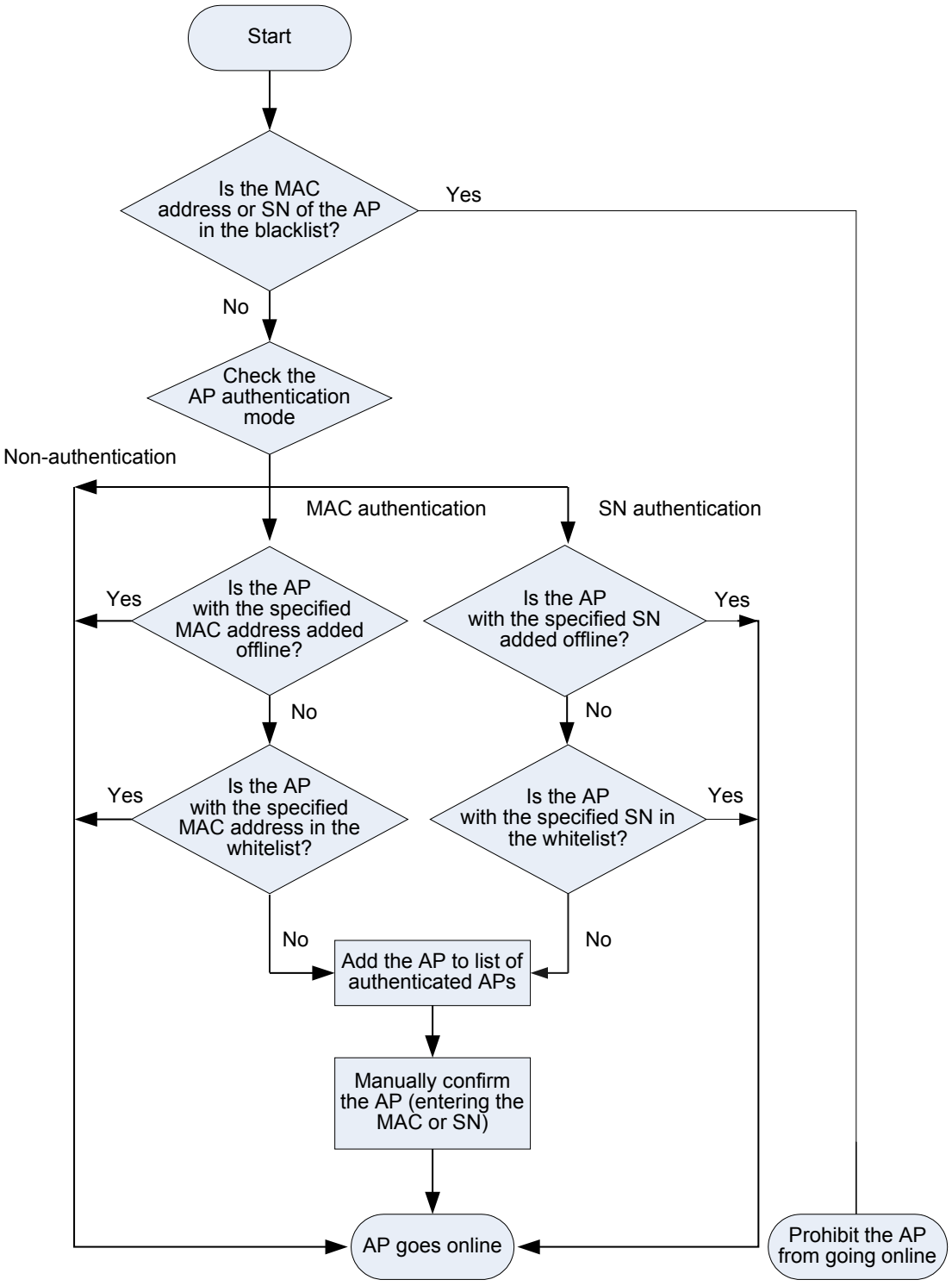
   For details about the setup of active and standby CAPWAP links, see **4.2.2 Dual-Link Backup**.

AP Access Control

The AP sends a Join Request packet to an AC. The AC then determines whether to allow the AP to access and sends a Join Response packet to the AP. The Join Response packet carries the AP software upgrade mode and AP version information.

Figure 1-9 shows the AP access control flowchart.

Figure 1-9 AP access control flowchart



(Optional) AP Software Upgrade

The AP determines whether its system software version is the same as that specified on the AC according to parameters in the received Join Response packet. If the two versions are different, the AP updates its software version in AC, FTP, or SFTP mode.

After the software version is updated, the AP restarts and repeats steps 1 to 3.

CAPWAP Tunnel Maintaining

The AP and AC exchange Keepalive packets to detect the data tunnel connectivity.

The AP and AC exchange Echo packets to detect the control tunnel connectivity.

AC Configuration Delivery

The AP sends a Configuration Update Request packet to the AC, which then replies with a Configuration Update Response packet to deliver the AP's service configuration to the AP.

1.2.5 STA Access

STAs can access wireless networks after CAPWAP tunnels are established. STA access includes three phases: scanning, link authentication, and association.

Scanning

A STA can actively or passively scan wireless networks.

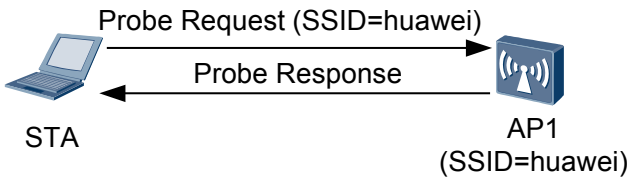
Active Scanning

In active scanning, a STA periodically searches for surrounding wireless networks. The STA can send two types of Probe Request frames: containing SSID and not containing SSID.

- The STA sends a Probe Request frame containing an SSID in each channel to search for the AP with the same SSID. Only the AP with the same SSID will respond to the STA. For example, in **Figure 1-10**, the STA sends a Probe Request frame containing SSID huawei to search for an AP with SSID huawei.

  This method applies to the scenario where a STA actively scans wireless networks to access a specified wireless network.

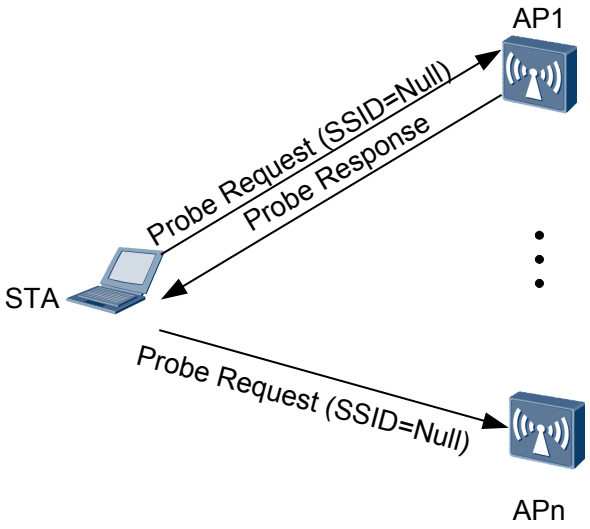
  Figure 1-10 Active scanning by sending a Probe Request frame containing an SSID

- The STA periodically broadcasts a Probe Request frame that does not contain an SSID in the supported channels as shown in **Figure 1-11**. The APs return Probe Response frames to notify the STA of the wireless services they can provide.

  This method applies to the scenario where a STA actively scans wireless networks to determine whether wireless services are available.

Figure 1-11 Active scanning by sending a Probe Request frame containing no SSID

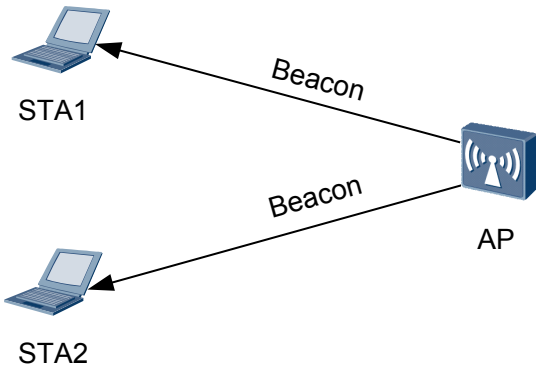


Passive Scanning

In **Figure 1-12**, a STA listens on the Beacon frames that an AP periodically sends in each channel to obtain AP information. A Beacon frame contains information including the SSID and supported rate.

To save power of a STA, enable the STA to passively scan wireless networks. In most cases, VoIP terminals passively scan wireless networks.

Figure 1-12 Passive scanning process

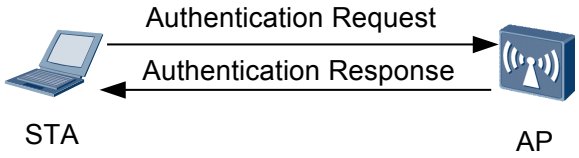


Link Authentication

To ensure wireless link security, an AP needs to authenticate STAs that attempt to access the AP. IEEE 802.11 defines two authentication modes: open system authentication and shared key authentication.

- Open system authentication: indicates no authentication, allowing any STA to associate with the AP, as shown in **Figure 1-13**.

Figure 1-13 Open system authentication



- Shared key authentication: requires that the STA and AP have the same shared key preconfigured. The AP checks whether the STA has the same shared key to determine whether the STA can be authenticated. If the STA has the same shared key as the AP, the STA can be authenticated. Otherwise, the STA cannot be authenticated.

Figure 1-14 Shared key authentication

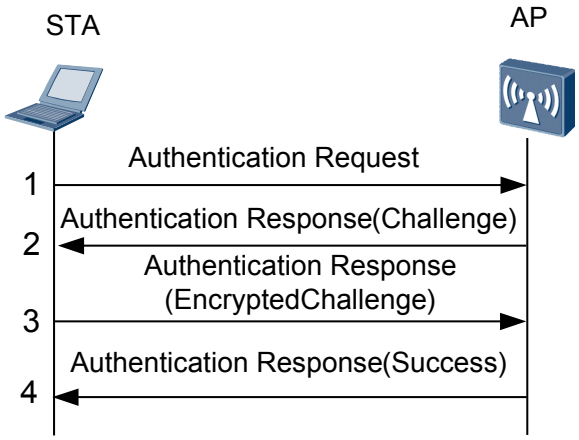


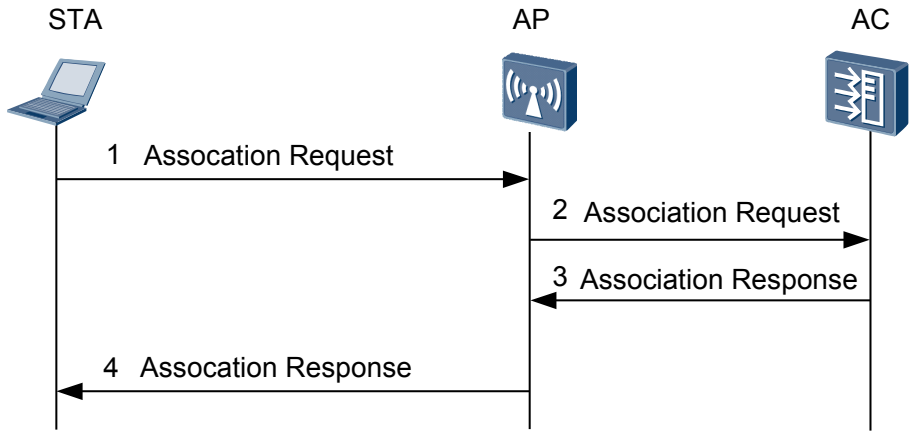
Figure 1-14 shows the shared key authentication process:

1. The STA sends an Authentication Request packet to the AP.
2. The AP generates a challenge and sends it to the STA.
3. The STA uses the preconfigured key to encrypt the challenge and sends it to the AP.
4. The AP uses the preconfigured key to decrypt the encrypted challenge and compares the decrypted challenge with the challenge sent to the STA. If the two challenges are the same, the STA can be authenticated. Otherwise, the STA cannot be authenticated.

Association

Client association refers to link negotiation. After link authentication is complete, a STA initiates link negotiation using Association packets, as shown in **Figure 1-15**.

Figure 1-15 STA association



NOTE

In **Figure 1-15**, the centralized WLAN architecture (AC+Fit AP) is used as an example to describe STA association. If the autonomous WLAN architecture (Fat AP) is used, steps 2 and 3 are performed on the Fat AP.

1. The STA sends an Association Request packet to the AP. The Association Request packet carries the STA's parameters and the parameters that the STA selects according to the service configuration, including the transmission rate, channel, QoS capabilities, access authentication algorithm, and encryption algorithm.
2. The AP receives the Association Request packet, encapsulates the packet into a CAPWAP packet, and sends the CAPWAP packet to the AC.
3. The AC determines whether to authenticate the STA according to the received Association Request packet and replies with an Association Response packet.
4. The AP decapsulates the received Association Response packet and sends it to the STA.

   NOTE

   The STA determines whether it needs to be re-authenticated according to the received Association Response packet:

   - If the STA does not need to be re-authenticated, the STA can access the wireless network.
   - If the STA needs to be re-authenticated, the STA initiates user access authentication. After being authenticated, the STA can access the wireless network. For details about user access authentication, see NAC in *Feature Description - Security*.

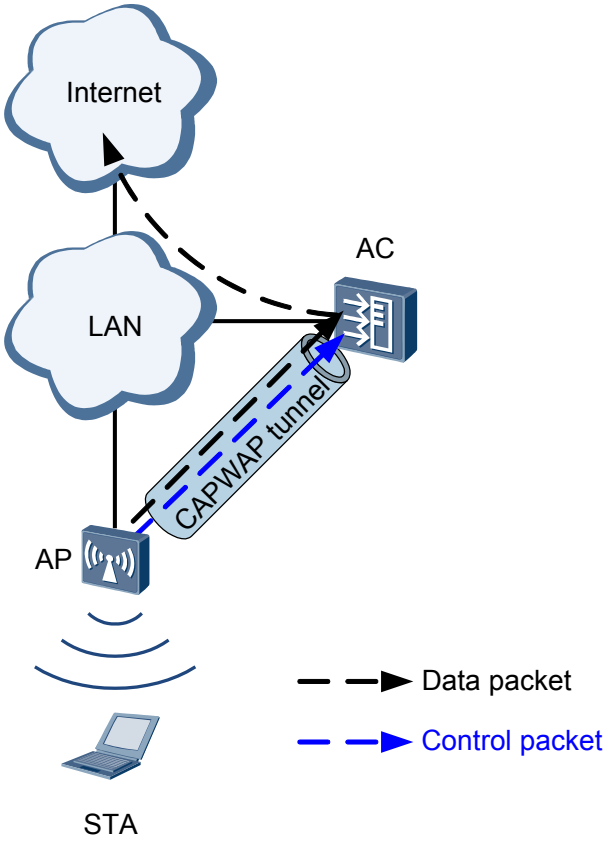
1.2.6 Data Forwarding Mode

Packets transmitted on a WLAN include control packets and data packets. Control packets are forwarded through CAPWAP control tunnels. Data packets are forwarded in tunnel forwarding (centralized forwarding) or direct forwarding (local forwarding) mode according to whether data packets are forwarded through CAPWAP data tunnels.

Tunnel Forwarding

In tunnel forwarding mode, APs encapsulate user data packets over a CAPWAP data tunnel and sends them to an AC, which then forwards these packets to an upper-layer network, as shown in **Figure 1-16**.

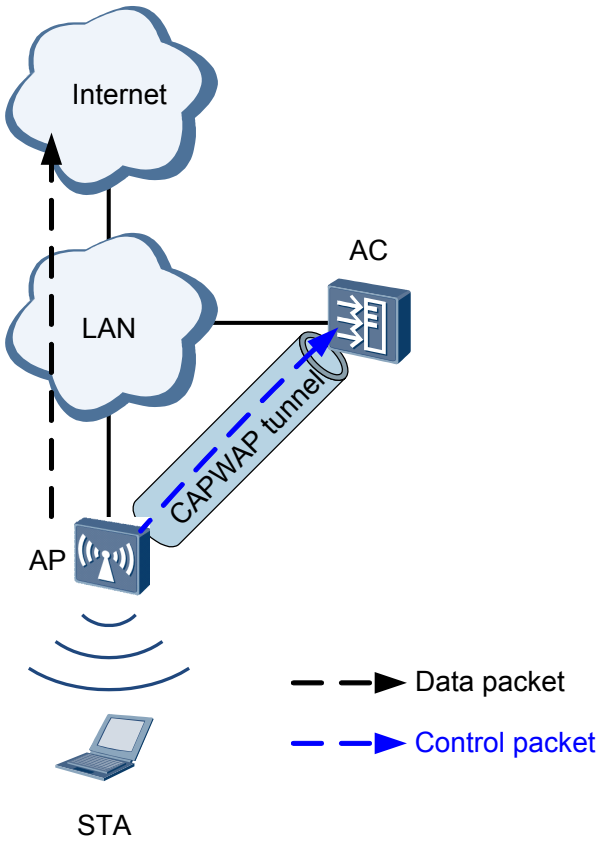
Figure 1-16 Tunnel forwarding



Direct Forwarding

In direct forwarding mode, an AP directly forwards user data packets to an upper-layer network without encapsulating them over a CAPWAP data tunnel, as shown in **Figure 1-17**.

Figure 1-17 Direct forwarding



Comparisons Between Tunnel forwarding and Direct forwarding

Table 1-3 lists the comparisons between tunnel forwarding and direct forwarding.

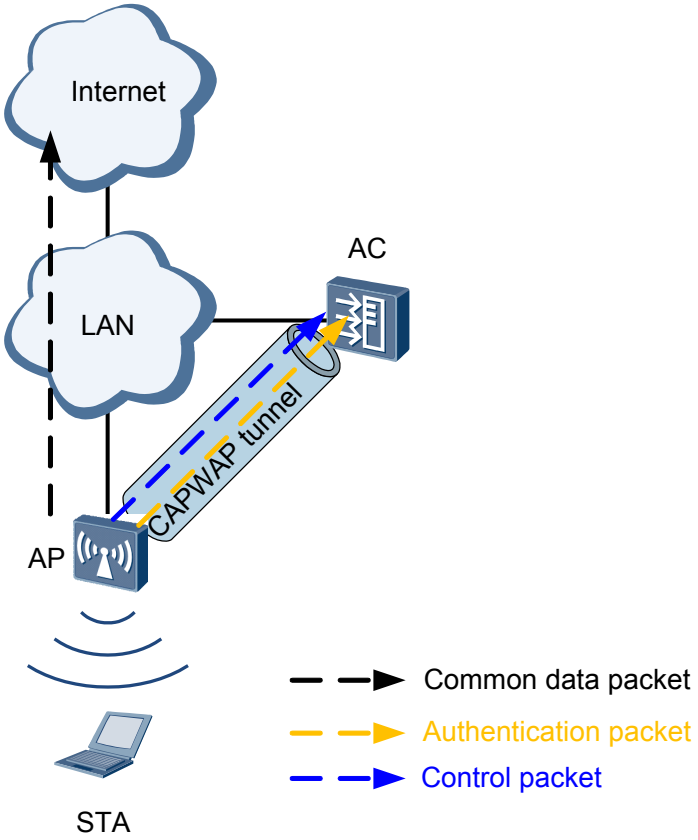
Table 1-3 Comparisons between tunnel forwarding and direct forwarding

Data Forwarding Mode	Advantage	Disadvantage
Tunnel forwarding	An AC forwards all data packets, ensuring security and facilitating centralized management and control.	User data must be forwarded by an AC, reducing packet forwarding efficiency and burdening the AC.
Direct forwarding	User data does not need to be forwarded by an AC, improving packet forwarding efficiency and reducing the burden on the AC.	User data is difficult to manage and control in a centralized manner.

Centralized Authentication in Direct Forwarding Mode

If direct forwarding is used, user data does not need to be forwarded by an AC. When user access authentication (for example, 802.1x authentication) is required on a wireless user access network and the access control point is deployed on an AC, user authentication packets cannot be managed by the AC in a centralized manner. This brings difficulties in controlling users in a uniform manner. Centralized authentication can be enabled in direct forwarding mode so that user authentication packets can be forwarded over CAPWAP tunnels to the AC, while common data packets do not need to be forwarded by the AC. **Figure 1-18** shows centralized authentication in direct forwarding mode.

Figure 1-18 Centralized authentication in direct forwarding mode



Centralized authentication and local forwarding implement 802.1X or Portal authentication on Layer 3 networks, and solve the following problems:

1. When an AC connects to an AP over a Layer 3 network and direct forwarding is used, 802.1x or Portal access control points cannot be deployed on the AC and the AC cannot control wireless access users in centralized manner. As a result, air interface control and user access control are separated.
2. When an AC connects to an AP over a Layer 3 network and direct forwarding is used, 802.1x or Portal access control points can be deployed on the switch. The management and maintenance costs are high. It is difficult to deploy and manage 802.1x access control points.
3. When an AC connects to an AP over a Layer 3 network and tunnel forwarding is used, 802.1x or Portal access control points can be deployed on the AC. All data is forwarded

through tunnels, and even local forwarding is limited by the bandwidth of the link between the AC and the AP.

1.3 Applications

1.3.1 WLAN Networking Application on Medium- and Large-sized Campus Networks

Medium and large campus networks are deployed in headquarters of large and medium enterprises, branches of large enterprises, colleges and universities, and airports. On a large campus network, a large number of APs are often deployed.

Most of these campus networks use the centralized WLAN architecture (AC+Fit AP) to facilitate network maintenance and enhance security. Based on the AC deployment mode, two AC solutions are available: centralized AC solution and distributed AC solution.

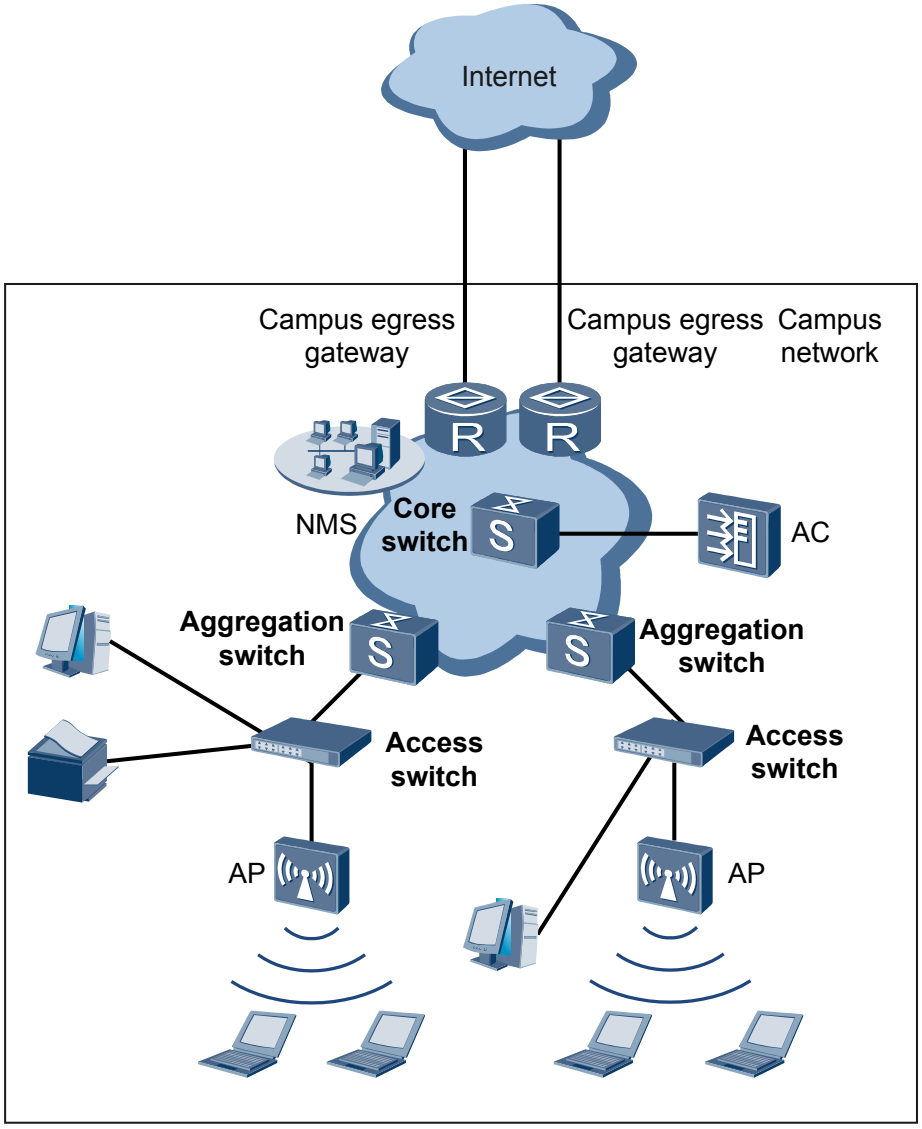
Centralized AC Solution

The centralized AC solution deploys independent ACs to manage APs on the network. An AC can be deployed in chain mode (between an AP and an aggregation or a core switch) or in branched mode (the AC is connected to only the aggregation or core switch).

- The chain mode applies to new WLANs.
- The branched mode applies to the scenario where the existing network topology remains unchanged and only ACs are deployed to meet WLAN requirements.

Figure 1-19 shows the centralized AC solution on a medium or large campus network. In **Figure 1-19**, the AC connects to only a core device.

Figure 1-19 Centralized AC solution on a medium or large campus network

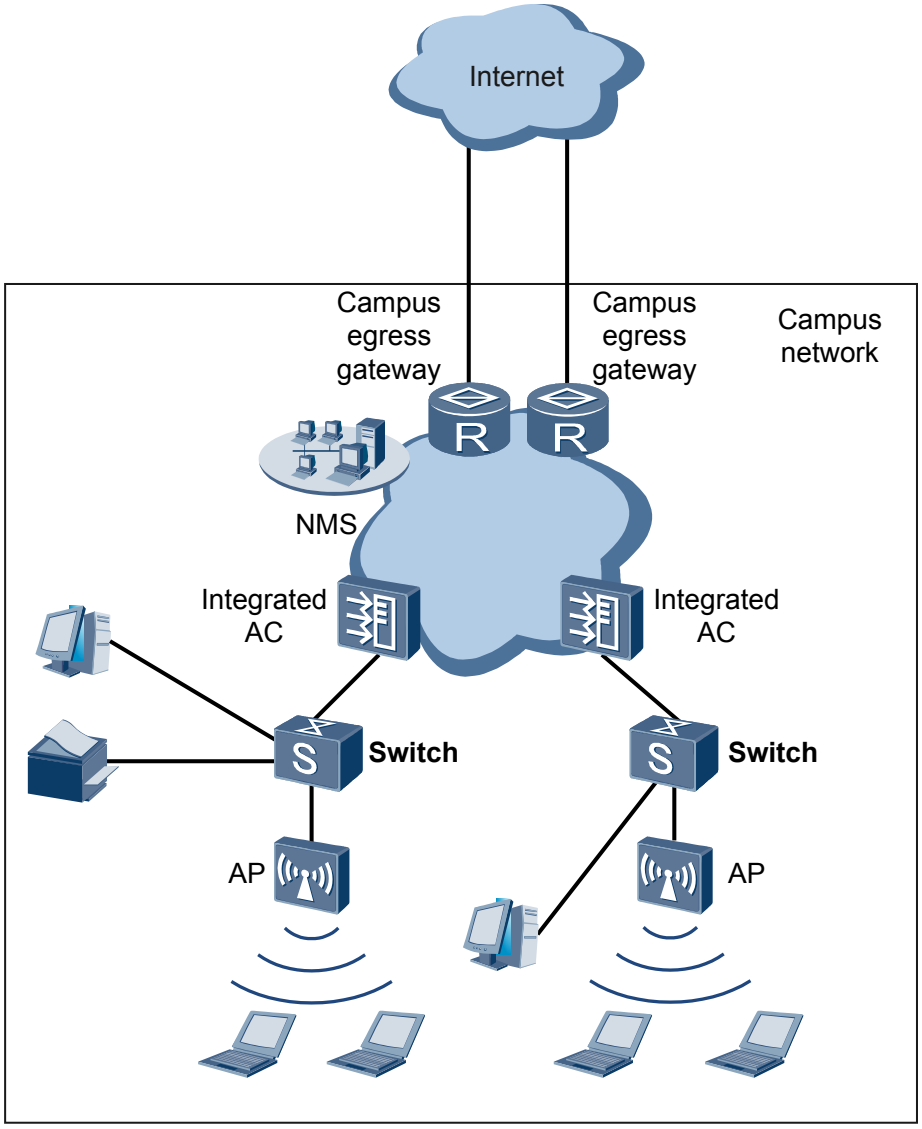


Distributed AC Solution

The distributed AC solution deploys multiple ACs in different areas to manage APs. This mode integrates AC functions on an aggregation switch to manage all the APs connected to the aggregation switch, without using an independent AC.

Figure 1-20 shows the distributed AC solution on a medium or large campus network.

Figure 1-20 Distributed AC solution on a medium or large campus network



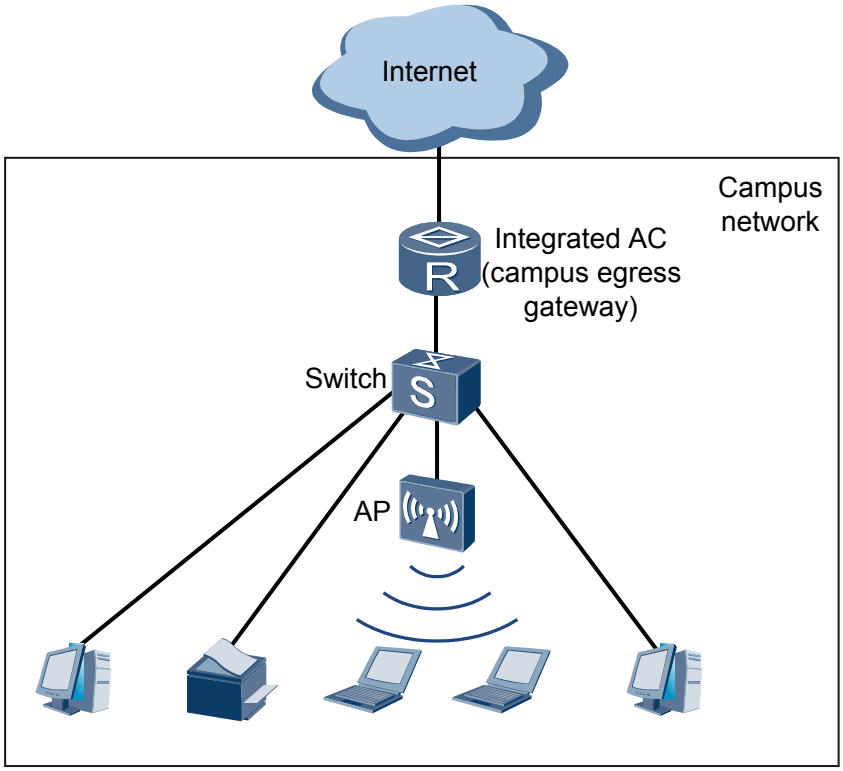
1.3.2 WLAN Networking Application on Small Campus Networks

Small-scale campus networks are deployed in small- and medium-scale enterprises. Its WLAN deployment scale is smaller than that on a large-scale campus network but is greater than that on a SOHO network.

To reduce costs, a small-scale campus network does not use dedicated NMS devices or authentication servers, resulting in low reliability.

A small-scale campus network often uses the centralized AC solution. You can use an independent AC or a router integrating AC functions to implement the centralized AC solution. In **Figure 1-21**, the router integrates AC functions to implement the centralized AC solution.

Figure 1-21 Small-scale campus network WLAN solution



1.3.3 WLAN Networking Application in Enterprise Branches

The enterprise branch WLAN networking can be used when an enterprise deploys WLANs in the headquarters and branches and the headquarters needs to manage WLANs in branches.

Large-scale and small-scale branch WLAN networkings are defined based on the AC deployment mode, independent of the network size. **Figure 1-22** and **Figure 1-23** show the large-scale and small-scale branch WLAN networkings.

Figure 1-22 Large-scale branch WLAN networking

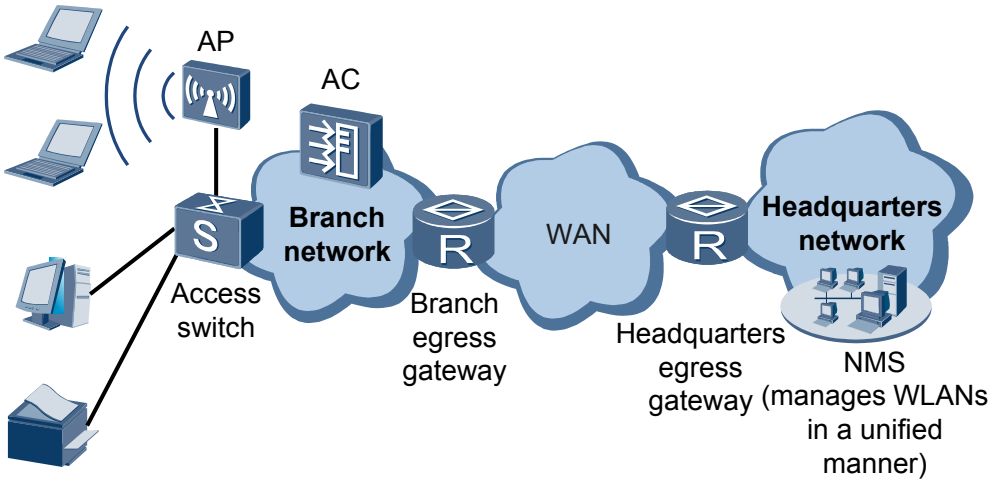
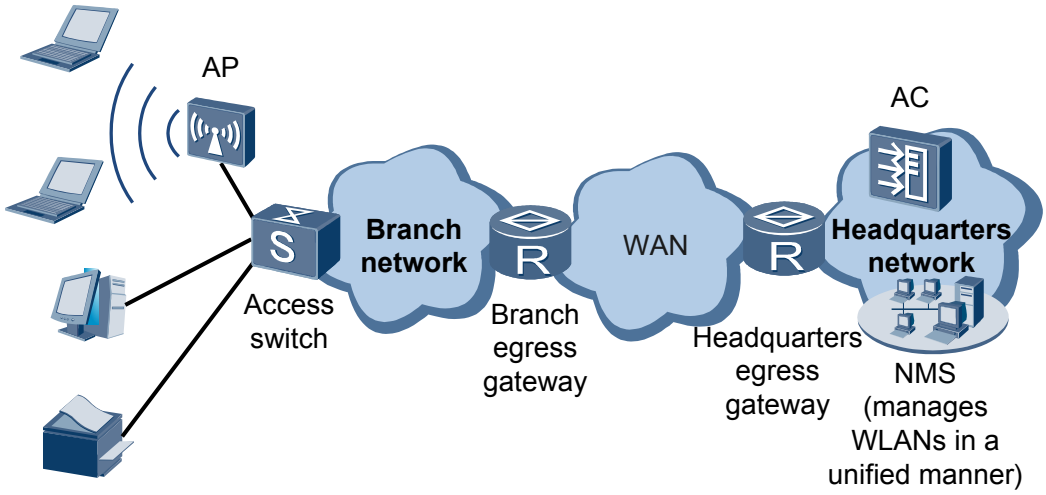


Figure 1-23 Small-scale branch WLAN networking

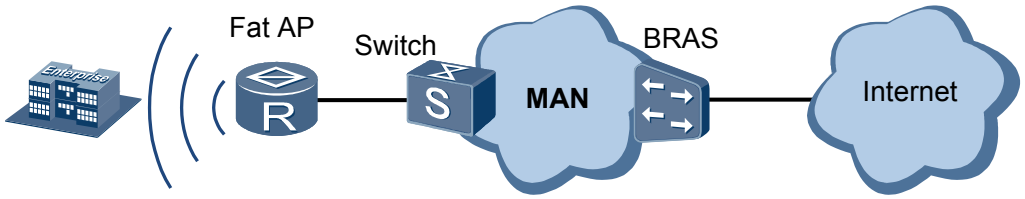


1.3.4 SOHO WLAN Networking Application

The SOHO WLAN solution applies to independent small-scale networks, for example, small-scale enterprises, stores, cafe bars, SOHO offices, or enterprise branches where WLAN services are deployed independently.

Most of SOHO WLAN networks have no independent authentication server or NMS device and use the autonomous architecture (Fat AP) without an AC. In **Figure 1-24**, an AR router is deployed on the SOHO WLAN to function as the Fat AP.

Figure 1-24 SOHO WLAN networking



1.4 References

The following table lists the references.

Document	Description	Remarks
RFC 5415	Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification	-

Document	Description	Remarks
RFC 5416	Control and Provisioning of Wireless Access Points Protocol Binding for IEEE 802.11	-
IEEE 802.11	WLAN communication standard	-
IEEE 802.1x	Standard for Port-based Network Access Control	-

2 WLAN Security

About This Chapter

2.1 Introduction to WLAN Security
2.2 Perimeter Security Principles
2.3 User Access Security Principles
2.4 Service Security Principles
2.5 Applications
2.6 References

2.1 Introduction to WLAN Security

Definition

WLAN security involves the following:

- Perimeter security: An 802.11 network is subject to threats from unauthorized APs and users, ad-hoc networks, and denial of service (DoS) attacks. A wireless intrusion detection system (WIDS) can detect unauthorized users and APs. A wireless intrusion prevention system (WIPS) can protect an enterprise network against unauthorized access from wireless networks.
- User access security: Link authentication, access authentication, and data encryption are used to ensure validity and security of user access on wireless networks.
- Service security: This feature protects service data of authorized user from being intercepted by unauthorized users during transmission.

Purpose

WLAN networks are easy to deploy and expand, flexible, and cost-effective. As WLAN technology uses radio signals to transmit service data, service data can easily be intercepted or tampered by attackers when being transmitted on the open wireless channels. Security has become a major factor that hinders WLAN technology development.

WLAN technology can provide the following mechanisms to guarantee data security for wireless users:

- WIDS and WIPS mechanisms that detect and defend against intrusion from unauthorized users
- Security policies for wireless users, including link authentication, access authentication, and data encryption
- Security mechanisms for wireless services, such as user isolation

2.2 Perimeter Security Principles

2.2.1 Wireless Intrusion Detection

Monitor APs can be configured on a network to prevent intrusion to the network. When configured with the intrusion detection function, monitor APs periodically listen on wireless signals. The AC can obtain information about wireless devices from the monitor APs and take countermeasures on unauthorized devices.

Before configuring intrusion detection on an AP, configure the working mode of the AP.

An AP supports three working modes: access mode, monitor mode, and hybrid mode:

- Access mode: If background neighbor probing is not enabled on an AP, the AP only transmits data of wireless users and does not monitor wireless users on the network. If

background neighbor probing is enabled, the AP can not only transmit data of wireless users but also scan wireless devices and listen on all 802.11 frames on wireless channels.

- Monitor mode: An AP scans wireless devices on the network and listens on all 802.11 frames on wireless channels. In this mode, all WLAN services on the AP are disabled and the AP cannot transmit data of wireless users.
- Hybrid mode: An AP can monitor wireless devices while transmitting data of wireless users.

  NOTE

  An AP can implement the WIDS or WIPS function only when it works in monitoring or hybrid mode.

  The configured WIDS or WIPS takes effect on an AP only after a service set is bound to the AP on the AC and the AC delivers the configurations to the AP.

Intrusion detection consists of two phases: wireless device identification and rogue device identification.

Wireless Device Identification

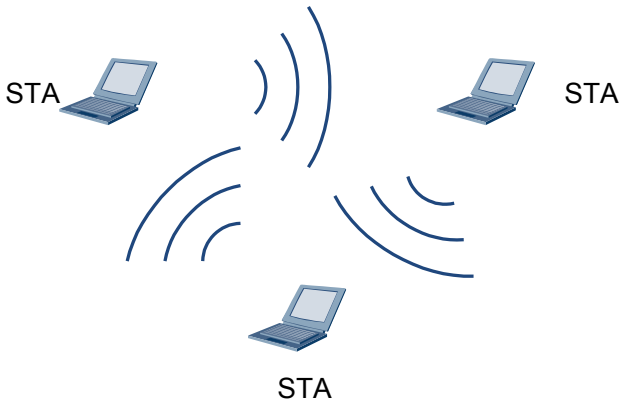
An AP working in monitoring or hybrid mode can identify types of neighboring wireless devices according to detected 802.11 management frames and data frames. The wireless device identification process is as follows:

1. The AP working mode is set to monitoring or hybrid on the AC.
2. The AC delivers the configuration to the AP.
3. The AP listens on frames sent from neighboring wireless devices to collect information about wireless devices. The AP determines frame types and device types according to MAC headers in received 802.11 MAC frames. For details about the 802.11 MAC frame format, see **1.2.2 802.11 Standards**.

   An AP can identify the following device types: AP, STA, wireless bridge, and ad-hoc device.

   - Wireless bridge: an AP provides wireless distribution system (WDS) service. For details about WDS, see **WLAN WDS**.
   - Ad-hoc device: a device on an ad-hoc network. An ad-hoc network is a temporary wireless network composed of several devices with wireless network adapters, as shown in **Figure 2-1**.

   Figure 2-1 Ad-hoc network

An AP identifies device types in the following way:

- When receiving a Probe Request, Association Request or Reassociation Request frame, the AP determines whether the sender is an ad-hoc device or STA according to the network type specified in the Frame Body field of the 802.11 MAC frame.
  - Ad-hoc: The network type is independent basic service set (IBSS).
  - STA: The network type is basic service set (BSS).
- When receiving a Beacon, Probe Response, Association Response, or Reassociation Response frame, the AP determines whether the sender is an ad-hoc device or AP according to the network type specified in the Frame Body field of the 802.11 MAC frame.
  - Ad-hoc: The network type is IBSS.
  - AP: The network type is BSS.
- The AP listens on all 802.11 data frames and checks the DS fields of the data frames to determine whether the sender is an ad-hoc device, wireless bridge, STA, or AP.
  - Ad-hoc device: In the Frame Control field of the 802.11 MAC header, both the To DS and From DS fields are 0.
  - Wireless bridge: In the Frame Control field of the 802.11 MAC header, both the To DS and From DS fields are 1.
  - STA: In the Frame Control field of the 802.11 MAC header, the To DS field is 1 and the From DS field is 0.
  - AP: In the Frame Control field of the 802.11 MAC header, the To DS field is 0 and the From DS field is 1.

Rogue Device Identification

Currently, an AC can identify only rogue APs.

APs periodically report collected device information to an AC, and the AC identifies rogue APs according to the reported device information.

1. The AC checks whether an AP is managed by itself. If so, the AC considers the AP an authorized device. If not, the AC goes to step 2.
2. The AC checks whether the AP is included in the whitelist of the SSID. If so, the AC considers the AP an authorized device. If not, the AC considers the AP a rogue AP.

   NOTE

   An AC can take a countermeasure on rogue APs to prevent STAs from associating with the rogue APs. For details about the countermeasure, see **2.2.2 Wireless Intrusion Prevention**.

2.2.2 Wireless Intrusion Prevention

An AC can prevent wireless intrusion of three types of unauthorized devices:

- Rogue AP

  After an AC identifies a rogue AP, it sends rogue AP information to a monitoring AP. The monitoring AP uses the rogue AP's identity information to broadcast a Deauthentication frame. After STAs that associate with the rogue AP receive the Deauthentication frame, they disassociate from the rogue AP. This countermeasure prevents STAs from associating with rogue APs.

NOTE

- Deauthentication frames are used to terminate established wireless links. Either an AP or a STA can send a Deauthentication frame to terminate the current link.
- Currently, an AC supports only countermeasure on rogue APs that have the same SSIDs as authorized APs managed by the AC.

- Unauthorized STA

  After an AC identifies an unauthorized STA, it sends unauthorized STA information to a monitoring AP. The monitoring AP uses the unauthorized STA's identity information to unicast a Deauthentication frame. After the AP with which the unauthorized STA associates receives the Deauthentication frame, the AP disassociates from the unauthorized STA. This countermeasure prevents APs from associating with unauthorized STAs.

- Ad hoc device

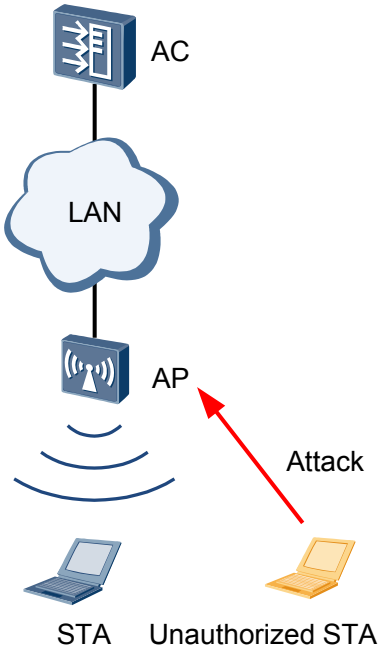
  After an AC identifies an ad hoc device, it sends the ad hoc device information to a monitoring AP. The monitoring AP uses the ad hoc device's identity information (BSSID and MAC address of the device) to unicast a Deauthentication frame. After the STAs that associate with the ad hoc device receive the Deauthentication frame, the STAs disassociate from the ad hoc device. This countermeasure prevents STAs from associating with ad hoc devices.

2.2.3 Attack Detection

On small- and medium-scale WLANs, the attack detection function can be enabled to detect flooding attacks, weak initialization vector (IV), and spoofing attacks. This function enables an AP to add attackers to the dynamic blacklist and send alarms to the AC to alert administrators.

Flooding Attack Detection

Figure 2-2 Flooding attack



In **Figure 2-2**, the AP receives a large number of management packets or empty data packets that have the same type and source MAC address within a short period. This is a flooding attack.

As a result, the system is busy processing these attack packets and cannot process packets from authorized STAs.

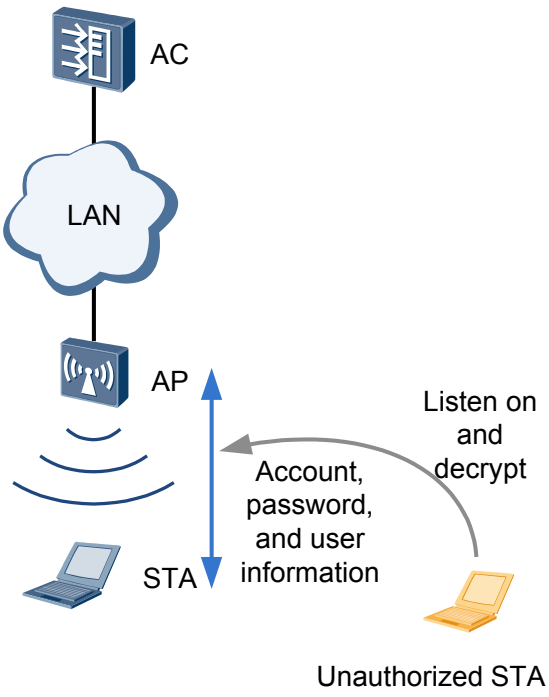
Flooding attack detection allows an AP to keep monitoring the traffic volume of each STA to prevent flooding attacks. When the traffic of a STA exceeds the allowed threshold (for example, the AP receives more than 100 packets from a STA within 1 second), the AP considers that the STA will flood packets and reports an alarm to the AC. If a dynamic blacklist is configured, the AP adds the detected attack device to the dynamic blacklist. Before the dynamic blacklist ages, the AP discards all the packets from the attack device to prevent the network from a flooding attack.

An AP can detect flooding attacks of the following packets:

- Authentication Request
- Deauthentication
- Association Request
- Disassociation
- Probe Request
- Action
- EAPOL Start
- EAPOL-Logoff
- PS-Poll
- RTS/CTS
- 802.11 Null

Weak IV Detection

Figure 2-3 Weak IV

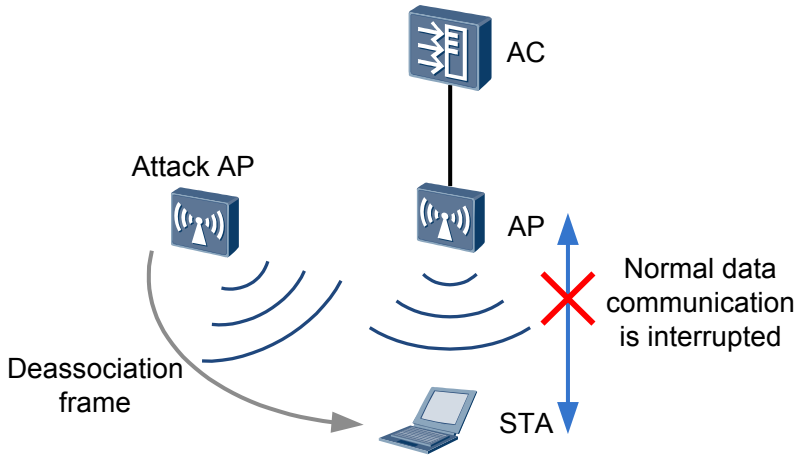


In **Figure 2-3**, when WEP encryption is used, a STA uses a 3-byte IV and a fixed shared key to encrypt each packet to be sent so that the same shared key generates different encryption effects. If the STA uses the weak IV (the first byte of the IV ranges from 3 to 15 and the second byte is 255), attackers can easily decrypt the shared key and access network resources because the IV of the packet sent by the STA is sent in plain text as one part of the header.

Weak IV detection identifies the IV of each WEP packet to prevent attackers from decrypting the shared key. When the AP detects a packet carrying the weak IV, the AP sends an alarm to the AC so that users can use other security policies to prevent STAs from using the weak IV for encryption.

Spoofing Attack Detection

Figure 2-4 Spoofing attack



In **Figure 2-4**, an attacker (a rogue AP or malicious user) forges an authorized user to send spoofing attack packets to STAs, which then fail to go online. This is a spoofing attack, which is also called man-in-the-middle attack. Spoofing attack packets includes broadcast Disassociation packets and Deauthentication packets.

After the spoofing attack detection function is enabled, an AP checks whether the source MAC address of a packet is its MAC address when receiving either of the two types of packets. If so, the WLAN is under the spoofing attack of Disassociation or Deauthentication packets.

2.2.4 Defense Against Brute Force Attacks on PSK

The brute force method is to search for a password by trying to use all possible password combinations. This method is also called the exhaustive attack method. For example, a 4-digit password that contains only digits may have a maximum of 10,000 combinations. The password can be decrypted after a maximum of 10,000 attempts. In theory, the brute force method can decrypt any password. The only problem is how to shorten the time used to decrypt a password. When a WLAN uses WPA/WPA2-PSK, WAPI-PSK, or WEP-Shared-Key as the security policy, attackers can use the brute force method to decrypt the password.

Defense against brute force attacks on PSK can prolong the time used to decrypt passwords to improve password security. An AP checks whether the number of key negotiation attempts during WPA/WPA2-PSK, WAPI-PSK, or WEP-Shared-Key authentication exceeds the configured threshold. If so, the AP considers that a user is using the brute force method to decrypt the password and reports an alarm to the AC. If the dynamic blacklist function is enabled, the

AP adds the user to the dynamic blacklist, discards all the packets of the user until the dynamic blacklist entry ages.

2.3 User Access Security Principles

2.3.1 Security Policy

Four WLAN security policies are available: Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), WPA2, WLAN Authentication and Privacy Infrastructure (WAPI). Each security policy has a series of security mechanisms, including the link authentication mechanism used to establish a wireless link, user authentication mechanism used when users attempt to connect to a wireless network, and data encryption mechanism used during data transmission.

2.3.1.1 WEP

Wired Equivalent Privacy (WEP), defined in IEEE 802.11, is used to protect data of authorized users from tampering during transmission on a WLAN. The WEP protocol uses the RC4 algorithm that encrypts data using a 64-bit or 128-bit encryption key. An encryption key contains a 24-bit initialization vector (IV) generated by the system, so the length of key configured on the WLAN server and client is 40 bits or 104 bits. WEP uses a static encryption key. That is, all STAs associating with the same SSID use the same key to connect to the wireless network.

A WEP security policy defines a link authentication mechanism and a data encryption mechanism.

Link authentication mechanisms include open system authentication and shared key authentication. For details about link authentication, see "Link Authentication" in **1.2.5 STA Access**.

- If open system authentication is used, data is not encrypted during link authentication. After a user goes online, service data can be encrypted by WEP or not, depending on the configuration.
- If shared key authentication is used, the WLAN client and server complete key negotiation during link authentication. After a user goes online, service data is encrypted using the negotiated key.

2.3.1.2 WPA/WPA2

WEP shared key authentication uses the RC4 symmetric stream cipher to encrypt data. This authentication method requires the same static key pre-configured on the server and client. Both the encryption mechanism and encryption algorithm can bring security risks to the network. The Wi-Fi Alliance developed Wi-Fi Protected Access (WPA) to overcome WEP defects before more secure policies are provided in 802.11i. WPA still uses the RC4 algorithm and defines the Temporal Key Integrity Protocol (TKIP) encryption algorithm. Later, 802.11i defined WPA2. Different from WPA, WPA2 uses an 802.1X authentication framework and supports Extensible Authentication Protocol-Protected Extensible Authentication Protocol (EAP-PEAP) and EAP-Transport Layer Security (EAP-TLS) authentication. In addition, WPA2 uses a more secure encryption algorithm: Counter Mode with CBC-MAC Protocol (CCMP).

Both WPA and WPA2 support 802.1X authentication and TKIP/CCMP encryption algorithm, ensuring better compatibility. The two protocols provide almost the same security level and their difference lies in the protocol packet format.

The WPA/WPA2 security policy involves four phases: link authentication, access authentication, key negotiation, and data encryption.

Link Authentication

Link authentication can be completed in open system authentication or shared key authentication mode. For details, see "Link Authentication" in **1.2.5 STA Access**.

WPA and WPA2 support only open system authentication.

Access Authentication

WPA and WPA2 have an enterprise edition and a personal edition.

- WPA/WPA2 enterprise edition (WPA/WPA2-802.1X authentication): uses a RADIUS server and the EAP protocol for authentication. Users provide authentication information, including the user name and password, and are authenticated by an authentication server (generally a RADIUS server).

  Large-scale enterprise networks usually use the WPA/WPA2 enterprise edition.

  NOTE

  For details about 802.1X authentication, see 802.1X Authentication in the *Feature Description - Security*.

  WPA/WPA2 implements 802.1X authentication using EAP-TLS and EAP-PEAP. **Figure 2-5** and **Figure 2-6** show EAP-TLS 802.1X authentication and EAP-PEAP 802.1X authentication processes.

Figure 2-5 EAP-TLS 802.1X authentication

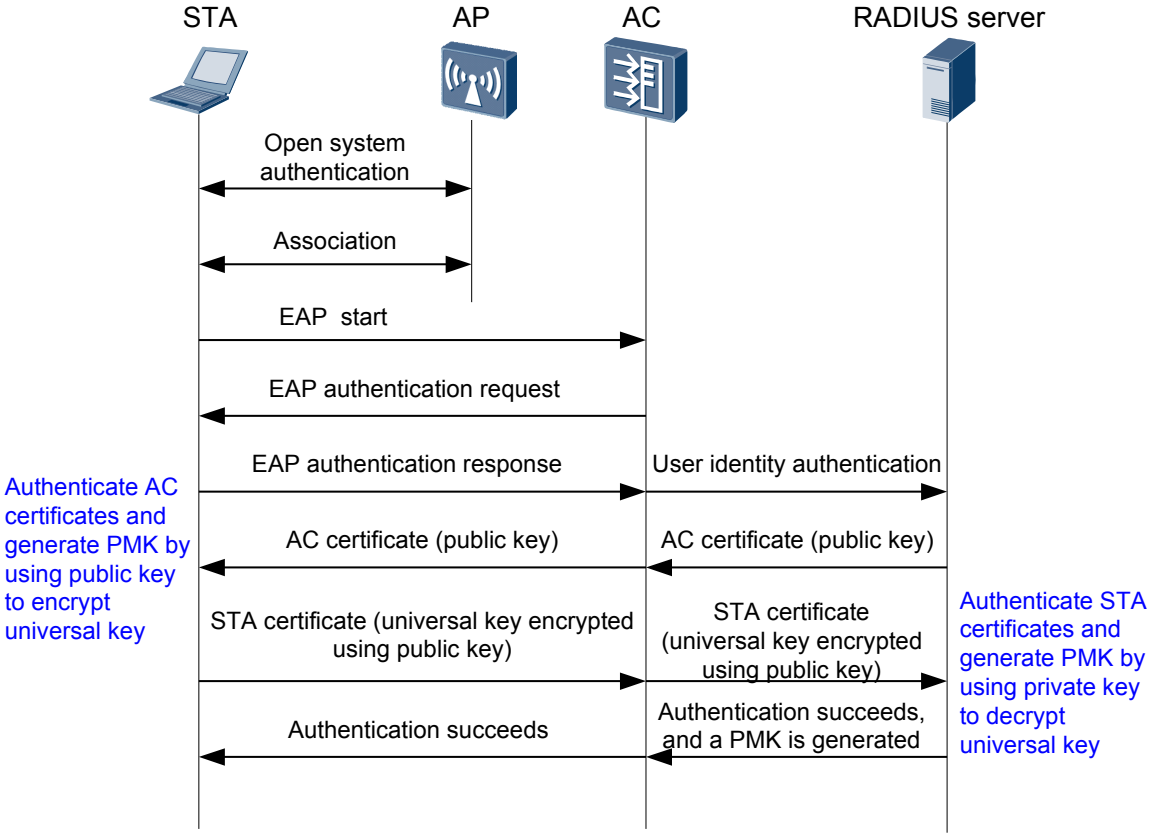
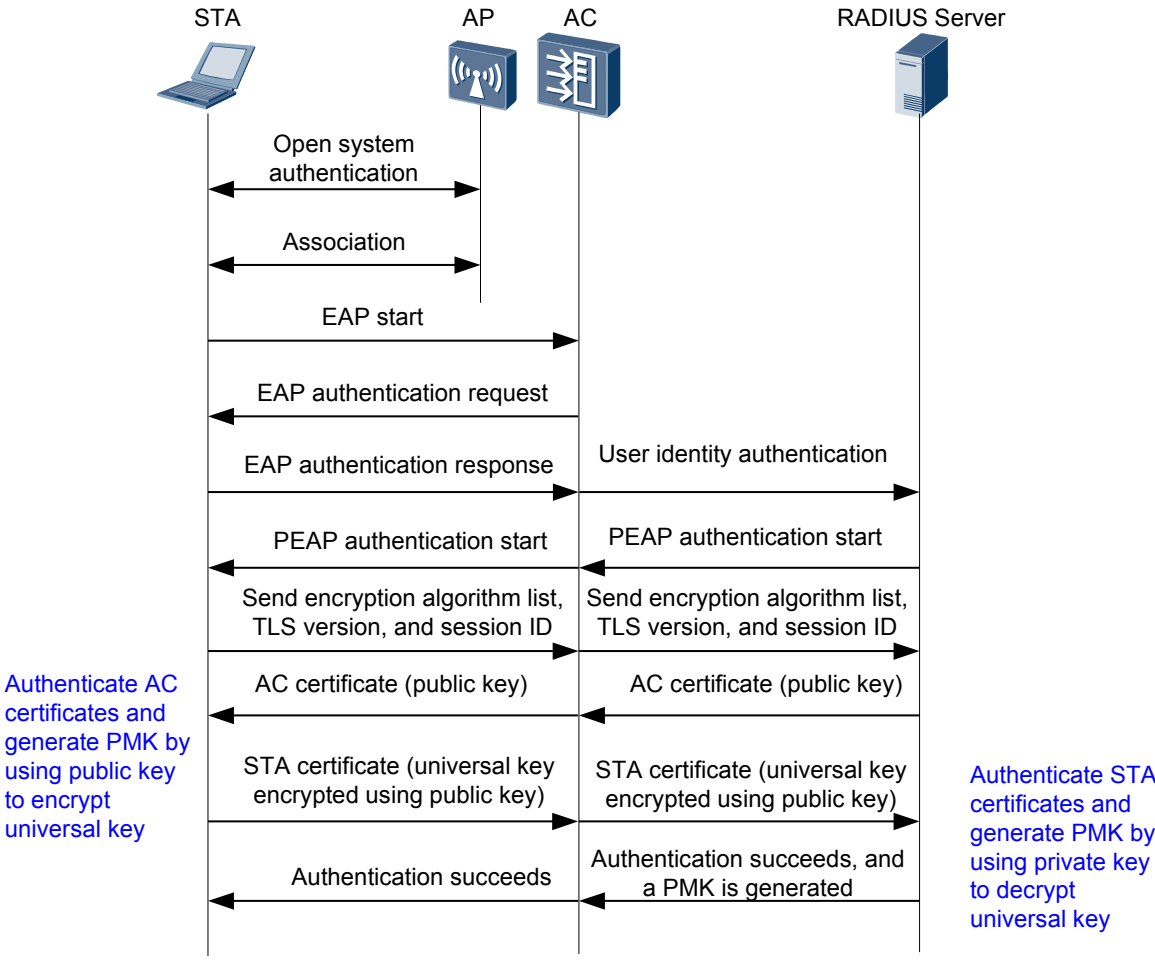


Figure 2-6 EAP-PEAP 802.1X authentication



- WPA/WPA2 personal edition: A dedicated authentication server is expensive and difficult to maintain for small- and medium-scale enterprises and individual users. The WPA/WPA2 personal edition provides a simplified authentication mode: pre-shared key (WPA-PSK) authentication. This mode does not require a dedicated authentication server. Users only need to set a pre-shared key on each WLAN node (including WLAN server, wireless router, and wireless network adapter). A WLAN client can access the WLAN if its pre-shared key is the same as that configured on the WLAN server. The pre-shared key is not used for encryption; therefore, it will not bring security risks like the 802.11 shared key authentication.

802.1X authentication can be used to authenticate wireless and wired users, whereas PSK authentication is specific to wireless users.

PSK authentication requires that a STA and an AC be configured with the same pre-shared key. The STA and AC authenticate each other through key negotiation. During key negotiation, the STA and AC use their pre-shared keys to decrypt the message sent from each other. If the messages are successfully decrypted, the STA and AC have the same pre-shared key. If they use the same pre-shared key, PSK authentication is successful; otherwise, PSK authentication fails.

Key Negotiation

802.11i defines two key hierarchies: pairwise key hierarchy and group key hierarchy. The pairwise key hierarchy protects unicast data exchanged between STAs and APs. The group key hierarchy protects broadcast or multicast data exchanged between STAs and APs.

During key negotiation, a STA and an AC use the pairwise master key (PMK) to generate a pairwise transient key (PTK) and a group temporal key (GTK). The PTK is used to encrypt unicast packets, and the GTK is used to encrypt multicast and broadcast packets.

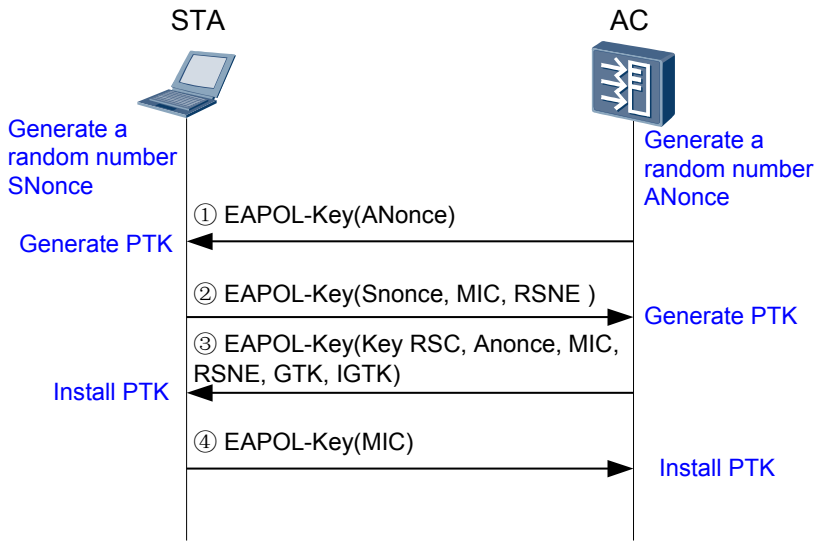
- In 802.1X authentication, a PMK is generated in the process shown in **Figure 2-5**.
- In PSK authentication, the method to generate a PMK varies according to the method to set the pre-shared key (configured using a command):
  - If the pre-shared key is a hexadecimal numeral string, it is used as the PMK.
  - If the pre-shared key is a character string, the PMK is calculated using the hash algorithm based on pre-shared key and service set identifier (SSID).

Key negotiation consists of unicast key negotiation and group key negotiation.

- Unicast key negotiation

  Key negotiation is completed through a four-way handshake between a STA and an AC, during which the STA and AC send EAPOL-Key frames to exchange information, as shown in **Figure 2-7**.

Figure 2-7 Unicast key negotiation



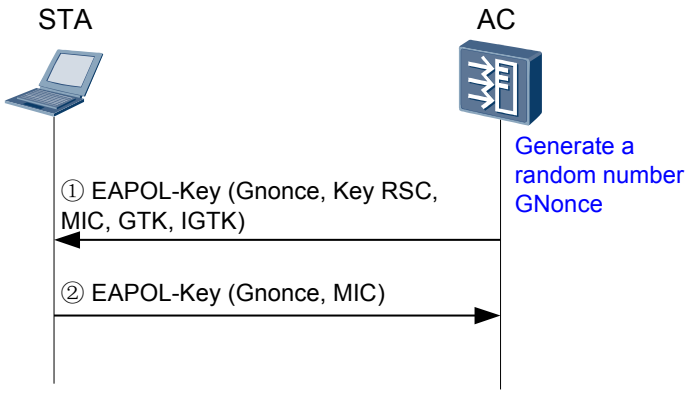
1. The AC sends an EAPOL-Key frame with a random value (ANonce) to the STA.
2. The STA calculates the PTK using MAC addresses of its own and the AC, PMK, ANonce, and SNonce, and sends an EAPOL-Key frame to the AC. The EAPOL-Key frame carries the SNonce, robust security network (RSN) information element, and message integrity code (MIC) of the EAPOL-Key frame. The AC calculates the PTK using the MAC addresses of its own and the STA, PMK, ANonce, and SNonce, and validates the MIC to determine whether STA's PMK is the same as its own PMK.

3. The AC sends an EAPOL-Key frame to the STA to request the STA to install the PTK. The EAPOL-Key frame carries the ANonce, RSN information element, MIC, and encrypted GTK.
4. The STA sends an EAPOL-Key frame to the AC to notify the AC that the PTK has been installed and will be used. The AC installs the PTK after receiving the EAPOL-Key frame.

- Group key negotiation

  Multicast key negotiation is completed through a two-way handshake. The two-way handshake begins after the STA and AC generate and install a PTK through a four-way handshake. **Figure 2-8** shows the two-way handshake process.

  Figure 2-8 Group key negotiation



1. The AC calculates the GTK, uses the unicast key to encrypt the GTK, and sends an EAPOL-Key frame to the STA.
2. After the STA receives the EAPOL-Key frame, it validates the MIC, decrypts the GTK, installs the GTK, and sends an EAPOL-Key ACK frame to the AC. After the AC receives the EAPOL-Key ACK frame, it validates the MIC and installs the GTK.

Data Encryption

WPA and WPA2 support TKIP and CCMP encryption algorithms.

- TKIP

  Unlike WEP that uses a static shared key, TKIP uses a dynamic key negotiation and management mechanism. Each user obtains an independent key through dynamic negotiation. The key of a user is calculated using the PTK generated in key negotiation, MAC address of the sender, and packet sequence number. This mechanism helps defend against attacks to WEP.

  TKIP uses MICs to ensure integrity of frames received on the receiver and validity of data sent by the sender and receiver. This mechanism protects information integrity. A MIC is calculated using the MIC key generated during key negotiation, destination MAC address, source MAC address, and data frame.

- CCMP

Different from WEP and TKIP that use a stream cipher algorithm, CCMP uses an Advanced Encryption Standard (AES) block cipher. The block cipher algorithm overcomes defects of the RC4 algorithm and provides a higher security.

2.3.1.3 WAPI

WLAN Authentication and Privacy Infrastructure (WAPI) is a Chinese national standard for WLANs, which was developed based on IEEE 802.11. WAPI provides higher security than WEP and WPA and consists of the following:

- WLAN Authentication Infrastructure (WAI): authenticates user identities and manages keys.
- WLAN Privacy Infrastructure (WPI): protects data transmitted on WLANs and provides the encryption, data verification, and anti-replay functions.

WAPI uses the elliptic curve cryptography (ECC) algorithm based on the public key cryptography and the block key algorithm based on the symmetric-key cryptography. The ECC algorithm is used for digital certificate authentication and key negotiation between wireless devices. The block key algorithm is used to encrypt and decrypt data transmitted between wireless devices. The two algorithms implement identity authentication, link authentication, access control, and user information encryption.

WAPI has the following advantages:

- Bidirectional identity authentication

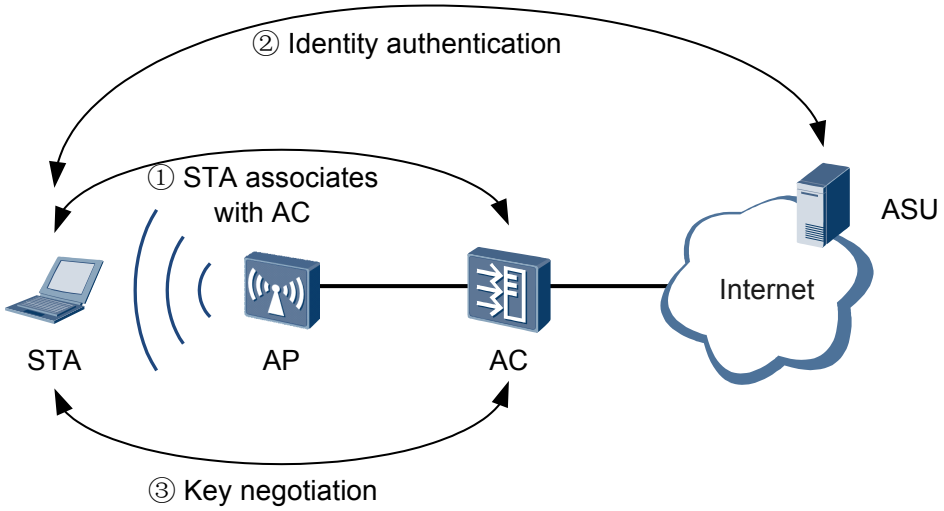
  Bidirectional identity authentication prevents access from unauthorized STAs and protects a WLAN against attacks from unauthorized WLAN devices. Other security policies only enable WLAN devices to authenticate STAs and do not provide a mechanism to authenticate WLAN devices.
- Digital certificate as identity information

  A WAPI system has an independent certificate server. STAs and WLAN devices use digital certificates to prove their identities, improving network security. When a STA requests to join or leave a network, the administrator only needs to issue a certificate to the STA or revoke the certificate of the STA.
- Well-developed authentication protocol

  WAPI uses digital certificates to identify STAs and wireless devices. During identity authentication, the elliptic curve digital signature algorithm is used to verify a digital certificate. In addition, the secure message hash algorithm is used to ensure message integrity, preventing attackers from tampering or forging information transmitted during identity authentication. In other security policies, the message integrity check mechanism is ineffective and cannot prevent attackers from tampering or forging authentication success messages.

As shown in **Figure 2-9**, WAPI involves identity authentication and key negotiation, which begin after a STA associates with an AC.

Figure 2-9 WAPI networking



Identity Authentication

WAPI provides two identity authentication modes: certificate-based mode (WAPI-CERT) and pre-shared key-based mode (WAPI-PSK).

- WAPI-CERT: A STA and an AC authenticate each other's certificate. The certificates must be loaded on the STA and AC and verified by an authentication service unit (ASU). After certificate authentication is complete, the STA and AC use the temporal public key and private key to generate a base key (BK) for key negotiation.

  The WAPI-CERT mode is applicable to large-scale enterprise networks or carrier networks that can deploy and maintain an expensive certificate system.

  Figure 2-10 WAPI certificate authentication

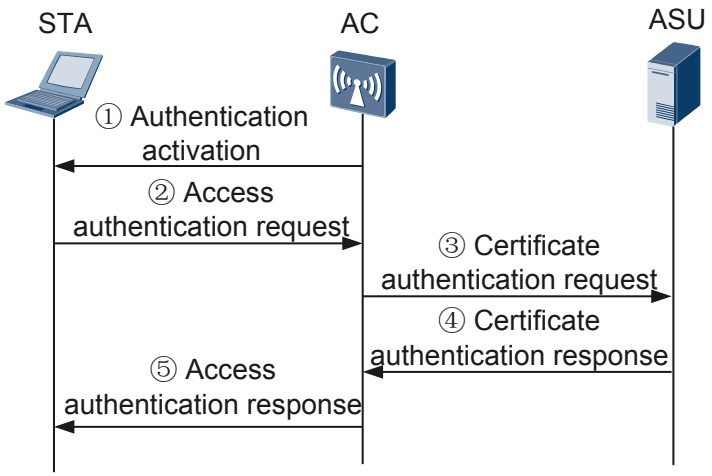
  

  Figure 2-10 shows the WAPI certificate authentication process.

  1. Authentication activation: When a STA requests to associate or re-associate with an AC, the AC checks whether the user is a WAPI user. If the user is a WAPI user, the

AC sends an authentication activation packet to trigger the certificate authentication process.

2. Access authentication request: The STA sends an access authentication request carrying the STA's certificate and system time to the AC. The system time is the access authentication request time.
3. Certificate authentication request: When the AC receives the access authentication request, it records the access authentication request time and sends a certificate authentication request to the ASU. The certificate authentication request carries the STA's certificate, access authentication request time, AC's certificate, and signature generated using the AC's private key and the preceding information.
4. Certificate authentication response: When the ASU receives the certificate authentication request, it authenticates the AC's signature and certificate. If the AC's signature and certificate are invalid, the authentication fails. If they are valid, the ASU authenticates the STA's certificate. After the authentication is complete, the ASU constructs a certificate authentication response with the STA's certificate authentication result, AC's certificate authentication result, and signature generated using the authentication results, and sends the certificate authentication response to the AC.
5. Access authentication response: When the AC receives the certificate authentication response, it checks the signature to obtain the STA's certificate authentication result, and controls access of the STA based on the certificate authentication result. The AC then forwards the certificate authentication response to the STA. The STA checks the signature generated by the ASU to obtain the AC's certificate authentication result, and determines whether to associate with the AC based on the result. If the certificate authentication succeeds, the AC accepts the access request. If the certificate authentication fails, the AC disassociates the STA from the network.

- WAPI-PSK: The STA and AC have the same pre-shared key configured before authentication. The pre-shared key is converted into a BK during authentication.

  The WAPI-PSK mode does not require an expensive certificate system, so it is applicable to individual users or small-scale enterprise networks.

Key Negotiation

After the AC is authenticated by the ASU, the AC initiates key negotiation with the STA. Key negotiation consists of unicast key negotiation and multicast key negotiation.

- Unicast key negotiation

  The STA and AC use the unicast encryption key and unicast integrity key obtained through unicast key negotiation to ensure security of unicast data exchanged between them. During unicast key negotiation, the STA and AC use the KD-HMAC-SHA256 algorithm to calculate a unicast session key (USK) based on the BK. In addition to the USK, the STA and AC also negotiate the encryption key and identity key used to generate the multicast key.

Figure 2-11 WAPI unicast key negotiation

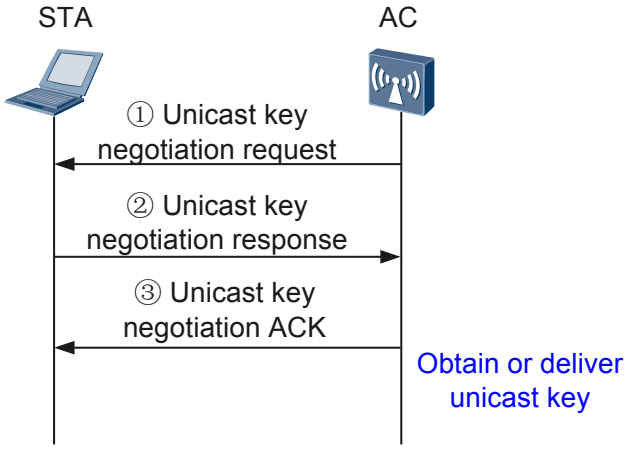


Figure 2-11 shows the unicast key negotiation process.

1. Unicast key negotiation request

   After a BK is generated, the AC sends a unicast key negotiation request packet to the STA.

2. Unicast key negotiation response

   After the STA receives the unicast key negotiation request packet, it performs the following steps:

   a. Checks whether this negotiation process is triggered to update the unicast key.
      - If so, the STA proceeds to step b.
      - If not, the STA proceeds to step c.

      NOTE

      WAPI allows the STA to directly send a unicast key negotiation response to the AC to initiate a unicast key update.

   b. Checks whether the challenge of the AC is the same as the challenge that is obtained in last unicast key negotiation and saved locally. If the two challenges are different, the STA drops the unicast key negotiation request packet.

   c. Generates a random challenge, and then uses the KD-HMAC-SHA256 algorithm to calculate a USK and the AC's challenge used for the next unicast key negotiation based on the BK, AC's challenge, and STA's challenge.

   d. Uses the message authentication key and HMAC-SHA256 algorithm to calculate a message authentication code, and sends it to the AC with a unicast key negotiation response packet.

3. Unicast key negotiation ACK

   After the AC receives the unicast key negotiation response packet, it performs the following steps:

   a. Checks whether the AC's challenge is correct. If the AC's challenge is incorrect, the AC drops the unicast key negotiation response packet.

   b. Uses the KD-HMAC-SHA256 algorithm to calculate a USK and the AC's challenge used for the next unicast key negotiation based on the BK, AC's challenge, STA's challenge. The AC then calculates the local message

authentication code using the message authentication key and HMAC-SHA256 algorithm, and compares the local message authentication code with that in the received unicast key negotiation response packet. If the two message authentication codes are different, the AC drops the unicast key negotiation response packet.

c. Checks the WAPI information element in the response packet if this is the first unicast key negotiation after the BK is generated. If the network type is BSS, the AC checks whether the WAPI information element in the response packet is the same as that in the association request packet it received before. If they are different, the AC sends a Deauthentication frame to disassociate the STA. If the network type is IBSS (ad-hoc network), the AC checks whether the unicast key algorithm supports the information element in the response packet. If not, the AC sends a Deauthentication frame to disassociate the STA.

d. Uses the message authentication key and HMAC-SHA256 algorithm to calculate a message authentication code, and sends it to the STA with a unicast key negotiation ACK packet.

- Multicast key negotiation

  The AC uses the multicast encryption key and multicast integrity key derived from the multicast master key (MMK) to encrypt broadcast or multicast data it sends, and sends a multicast key advertisement packet to the STA. The STA obtains the multicast encryption key and multicast integrity key from the multicast key advertisement packet to decrypt the broadcast or multicast data it receives.

  Multicast key negotiation is performed after unicast key negotiation is complete. The AC advertises the multicast keys to the STA in this process.

Figure 2-12 WAPI multicast key negotiation

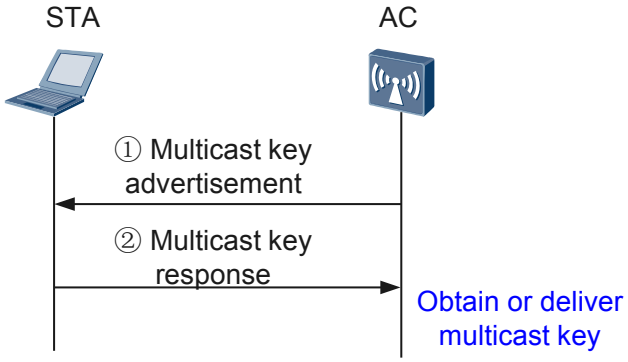


Figure 2-12 shows the multicast key negotiation process.

1. Multicast key advertisement

   The AC uses the random number algorithm to calculate a MMK, encrypts the MMK using the negotiated unicast key, and sends an advertisement packet to notify the STA of the MMK.

2. Multicast key response

   After the STA receives the multicast key advertisement packet, it performs the following steps:

   a. Calculates the checksum using the message authentication key identified by the unicast key identifier, and compares the checksum with the message

authentication code. If the checksum is different from the message authentication code, the STA drops the multicast key advertisement packet.

b. Checks whether the key advertisement identifier is increasing. If not, the STA drops the multicast key advertisement packet.

c. Decrypts the multicast key to obtain the 16-byte master key and uses the KD-HMAC-SHA256 algorithm to extend it to 32 bytes. The first 16 bytes indicate the encryption key, and the last 16 bytes indicate the integrity key.

d. Saves the key advertisement identifier and sends a multicast key response packet to the AC.

After the AC receives the multicast key response packet, it performs the following steps:

a. Calculates the checksum using the message authentication key identified by the unicast key identifier, and compares the checksum with the message authentication code. If the checksum is different from the message authentication code, the AC drops the multicast key response packet.

b. Compares fields (such as key advertisement identifier) in the multicast key response packet with corresponding fields in the multicast key advertisement packet it has sent. If all the fields are the same, the multicast key negotiation is successful. Otherwise, the AC drops the multicast key response packet.

Key Update

WAPI defines a dynamic key negotiation mechanism, but there are still security risks if a STA uses the same encryption key for a long time. To enhance security, WAPI provides time-based and packet-based key updates mechanisms:

- Time-based key update: The unicast and multicast keys of a STA have an aging time (configured using a command). When the aging time of the current unicast or multicast key expires, the STA and AC negotiate a new unicast or multicast key.
- Packet-based key update: When the number of packets encrypted using a unicast or multicast key reaches a specified value (configured using a command), the STA and AC negotiate a new unicast or multicast key.

2.3.2 STA Blacklist and Whitelist

On a WLAN, blacklist or whitelist can be configured to filter access from STAs based on specified rules. The blacklist or whitelist allows authorized STAs to connect to the WLAN and rejects access from unauthorized STAs.

- Whitelist

  A whitelist contains MAC addresses of STAs that are allowed to connect to a WLAN. After the whitelist function is enabled, only the STAs in the whitelist can connect to the WLAN, and access from other STAs is rejected.

- Blacklist

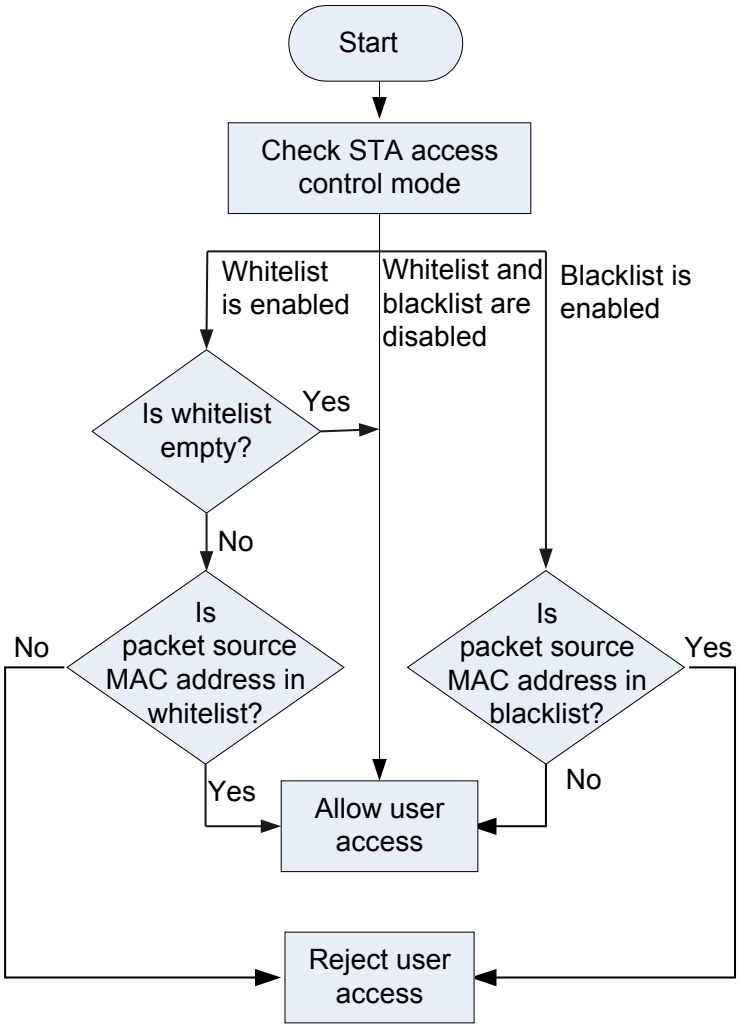
  A blacklist contains MAC addresses of STAs that are not allowed to connect to a WLAN. After the blacklist function is enabled, STAs in the blacklist cannot connect to the WLAN, and other STAs can connect to the WLAN.

NOTE

If the STA whitelist or blacklist function is enabled but the whitelist or blacklist is empty, all STAs can connect to the WLAN.

Figure 2-13 shows how STA blacklist and whitelist work.

Figure 2-13 STA blacklist and whitelist working process



2.4 Service Security Principles

2.4.1 User Isolation

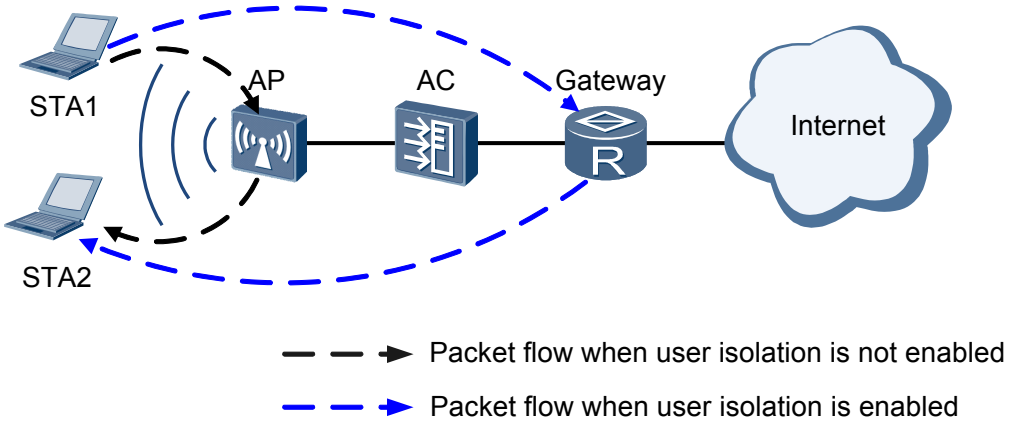
In public places (such as airports and cafes), carriers' networks, medium- and large-sized enterprises, and financial organizations, users may need to connect to the Internet wirelessly. In these scenarios, user isolation can ensure security of data transmitted between users. User isolation can be implemented based on VAPs or user groups.

VAP-based User Isolation

In VAP-based user isolation mode, Layer 2 packets cannot be transmitted between WLAN users associating with the same VAP. All user traffic must be forwarded by the gateway, and all WLAN users communicate through the gateway.

As shown in **Figure 2-14**, STA1 and STA2 associate with the same VAP. Before user isolation is enabled, Layer 2 packets can be forwarded between STA1 and STA2. (Layer 2 packets are forwarded by the AP in direct forwarding mode and by the AC in tunnel forwarding mode.) After user isolation is enabled, Layer 2 packets cannot be forwarded between STA1 and STA2.

Figure 2-14 VAP-based user isolation (direct forwarding mode)



User Group-based User Isolation

WLAN users need to be dynamically authorized to limit the network resources users can access after they go online. A RADIUS server controls user authority based on user groups. After a user is authenticated, the RADIUS server delivers a user group for the user to the AC. User groups can be associated with different ACL rules to control authorization information for different types of users. User group-based user isolation can isolate users within a user group or between different user groups to protect security of service data.

After intra-group user isolation is configured in a user group, users in the user group cannot communicate with each other.

After inter-group isolation is configured in a user group, users in the user group cannot communicate with users in other user groups.

2.4.2 Terminal Type Identification

Bring Your Own Device (BYOD) has become a trend as the Internet develops fast. Many enterprises now allow employees to connect to enterprise networks wirelessly using their own mobile terminals, such as mobile phones, tablet computers, or laptops. This work style enables employees to use up-to-date technologies, gives them more flexibility in work, and improves their working efficiency. However, employees' own terminals may bring security risks to enterprise networks, and traditional security technology that authenticates and authorizes users based on user roles cannot secure enterprise networks in this scenario. Terminal type identification technology can solve this problem. This technology identifies types of mobile terminals that employees use to connect to an enterprise network to control access from the

mobile terminals. Enterprises can use this technology to implement user authentication and authorization based on user information, device type, access time, access location, and device operating environment.

Concepts

User Agent (UA): a field in a Hypertext Transfer Protocol (HTTP) header. A terminal type identification server can identify a terminal's operating system, operating system version, CPU type, browser, browser version, browser rendering engine, browser language, and browser plug-ins according to this field.

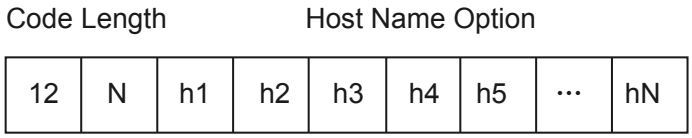
Terminal type identification: A terminal type identification server analyzes fields in packets sent from users to identify terminal types.

Implementation

The AC can identify terminal types by analyzing MAC addresses, UA information, and DHCP option information:

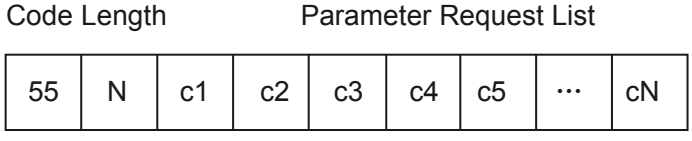
- A terminal's organizationally unique identifier (OUI), the first 12 bits in its MAC address, identifies the manufacturer of the terminal.
- The UA field in an HTTP packet sent from a terminal identifies the terminal's operating system, operating system version, CPU type, browser, and browser version.
- The Option 12, Option 55, or Option 60 field in a DHCP packet sent by a terminal identifies the host name of the terminal and manufacturer type.
  - As shown in **Figure 2-15**, DHCP Option 12 is the Host Name Option. In this option field, 12 indicates the information type, N indicates the length of the following information, and h1 to hN indicate the information content (containing the host name of the STA).

Figure 2-15 DHCP Option 12 format



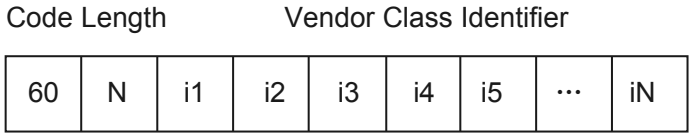
  - As shown in **Figure 2-16**, DHCP Option 55 is the Parameter Request List. In this option field, 55 indicates the information type, N indicates the length of the following information, and c1 to cN indicate the information content (containing the list of parameters requested by a STA). Different STAs may request different parameters.

Figure 2-16 DHCP Option 55 format



  - As shown in **Figure 2-17**, DHCP Option 60 is the Vendor Class Identifier. In this option field, 60 indicates the information type, N indicates the length of the following information, and i1 to iN indicate the information content (containing the manufacturer identifier).

Figure 2-17 DHCP Option 60 format



The AC can obtain the MAC address, DHCP option information, and UA information of a terminal during Portal or 802.1x authentication.

During Portal authentication, the AC identifies the type of a terminal as follows:

1. After a user successfully associates with an AP, the AC obtains the user MAC address.
2. When the user sends a DHCP Request packet to apply for an IP address, the AP uses the DHCP snooping function to obtain the option information from the DHCP Request packet and sends the option information to the AC.
3. When the user sends an HTTP Get packet to obtain the authentication page, the AC analyzes the HTTP Get packet and obtains the UA information from the packet.
4. An AC identifies the terminal type by analyzing the MAC address, UA information, and DHCP option information of the user.
5. The AC encapsulates the terminal type in an Authentication Request packet and sends the Authentication Request packet to the AAA server. The AAA server authenticates the user using the user account and terminal type, and delivers corresponding right to the user.

During 802.1x authentication, the AC identifies the type of a terminal as follows:

1. After a user successfully associates with an AP, the AC obtains the user MAC address.
2. The AC identifies the terminal type according to the OUI in the MAC address. If the OUI is an identifiable one, the AC encapsulates the terminal type in an Authentication Request packet and sends the Authentication Request packet to the AAA server.
3. When the user sends a DHCP Request packet to apply for an IP address, the AP uses the DHCP snooping function to obtain the option information from the DHCP Request packet and sends the option information to the AC.
4. The AC identifies the terminal type according to the MAC address and DHCP option information, encapsulates the terminal type in an accounting packet, and sends the accounting packet to the AAA server.
5. When the user sends an HTTP Get packet to obtain the authentication page in the redirection process, the AC analyzes the HTTP Get packet and obtains the UA information from the packet.
6. The AC identifies the terminal type according to the MAC address, UA information, and DHCP option information, encapsulates the terminal type in an accounting packet, and sends the accounting packet to the AAA server.

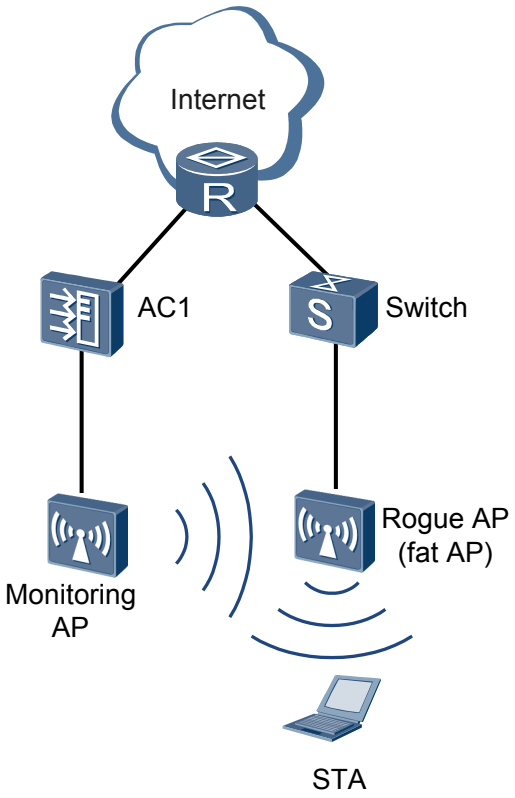
2.5 Applications

2.5.1 WIDS/WIPS

As shown in **Figure 2-18**, an employee connects to a rogue fat AP from the campus network or uses simulation software to simulate a fat AP. After wireless intrusion detection system (WIDS) and wireless intrusion prevention system (WIPS) are configured on AC1, the monitor AP collects

neighbor information and reports it to AC1. When AC1 identifies the rogue AP, AC1 notifies the monitor AP of the rogue AP's identity information. The monitor AP then uses the rogue AP's identity information to broadcast a Deauthentication frame. After STAs associating with the rogue AP receive the Deauthentication frame, they disassociate from the rogue AP. This countermeasure prevents STAs from associating with the rogue AP.

Figure 2-18 WIDS/WIPS networking



2.5.2 Security Policy

Commonly Used Security Policy for Households and SOHO Networks

Households and SOHO networks do not require high security. They usually use the WPA/WPA2 personal edition and do not require an authentication server.

Commonly Used Security for Enterprise Networks

Enterprise networks require high security. They usually use the 802.1X-based WPA/WPA2 enterprise edition and deploy an authentication server.

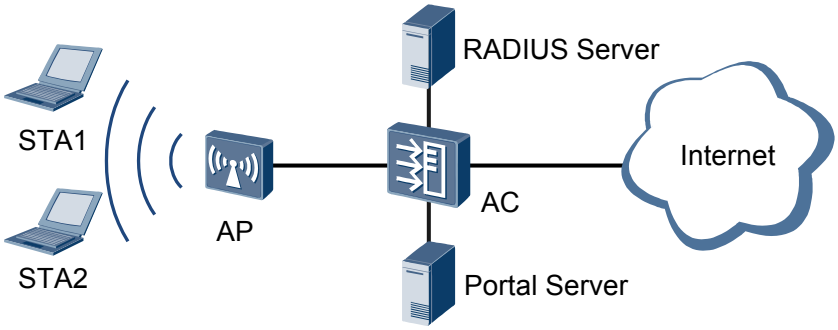
Commonly Used Security Policy for Carrier Networks

Besides WEP, WPA/WPA2, and WAPI that are specific to wireless users, carriers can combine WLAN security policies with port authentication to enhance security of wireless users. Port authentication methods include 802.1X authentication, MAC address authentication, and Portal

authentication. For details about the authentication methods, see NAC in the *Feature description - Security*.

As shown in **Figure 2-19**, a carrier WLAN network usually uses WEP (no authentication, no encryption) and Portal authentication. When a STA attempts to connect to wireless network, the AC pushes the Portal authentication web page to the user. The user must enter the user name and password on the displayed web page. If the user is successfully authenticated by the RADIUS server, the user can connect to the Internet wirelessly.

Figure 2-19 WEP+Portal authentication

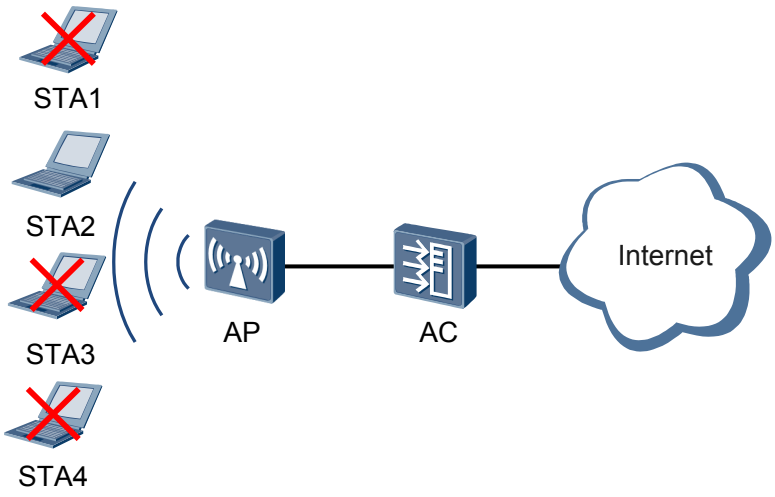


2.5.3 STA Blacklist and Whitelist

STA Whitelist

As shown in **Figure 2-20**, visiting employees often bring their laptops in an AP's coverage area on a campus network. If only STAs of a few local employees are allowed to connect to the wireless network, the enterprise can configure the whitelist function on the AC and add MAC addresses of these STAs to the whitelist. In this example, STA2 is added to the whitelist. Then only STA2 can connect to the wireless network, and STAs not in the whitelist (STA1, STA3, and STA4 in **Figure 2-20**) cannot connect to the wireless network through the AP.

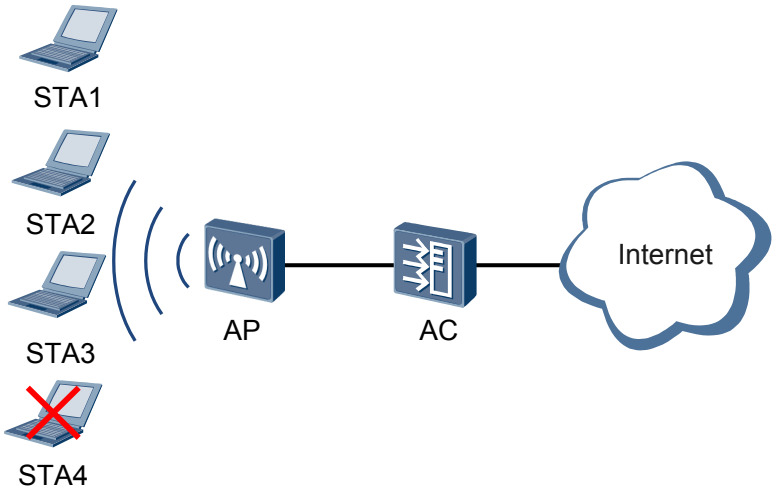
Figure 2-20 STA whitelist application



STA Blacklist

As shown in **Figure 2-21**, many STAs of local employees exist in an AP's coverage area on a campus network. Guests or visiting employees sometimes bring their laptops to this AP's coverage area. If only STAs of guests or visiting employees are not allowed to connect to the wireless network, the enterprise can configure the blacklist function on the AC and add MAC addresses of these STAs to the blacklist. In this example, STA4 is added to the blacklist. Then STA4 cannot connect to the wireless network through the AP, and other STAs (STA1, STA2, and STA3 in **Figure 2-21**) can connect to the wireless network.

Figure 2-21 STA blacklist application



2.6 References

The following table lists the reference for this feature.

Document	Description	Remarks
IEEE 802.11i	Medium Access Control (MAC) Security Enhancements	-

3 Radio Resource Management

About This Chapter

3.1 Introduction to Radio Resource Management

3.2 Principles

3.3 References

3.1 Introduction to Radio Resource Management

Definition

Radio resource management enables APs to check the surrounding radio environment, dynamically adjust working channels and transmit power, and evenly distribute access users. This function helps reduce radio signal interference, adjust radio coverage, and enable a wireless network to quickly adapt to changes in the radio environment. With the radio resource management function, the wireless network can provide high service quality for wireless users and maintain an optimal radio resource utilization.

Purpose

WLAN technology uses radio signals (such as 2.4 GHz or 5 GHz radio waves) as transmission medium. Radio waves will attenuate when they are transmitted over air, degrading service quality for wireless users. Radio resource management enables a WLAN to adapt to changes in the radio environment by dynamically adjusting radio resources. This improves service quality for wireless users.

3.2 Principles

3.2.1 Radio Calibration

Overview

On a WLAN, operating status of APs is affected by the radio environment. For example, adjacent APs using the same working channel interfere with each other, and a large-power AP can interfere with adjacent APs if they work on overlapping channels. The radio calibration function can dynamically adjust channels and power of APs managed by the same AC to ensure that the APs work at the optimal performance.

- Channel adjustment

  On a WLAN, adjacent APs must work on non-overlapping channels to avoid radio interference. For example, the 2.4 GHz frequency band is divided into 14 overlapping 20 MHz channels, as shown in **Figure 3-1**.

  NOTE

  For channels supported in different countries, see the *Country Code & Channel Compliance Table*.You can search and obtain this table at *http://support.huawei.com/enterprise*.

  Figure 3-1 Channels in the 2.4 GHz frequency band

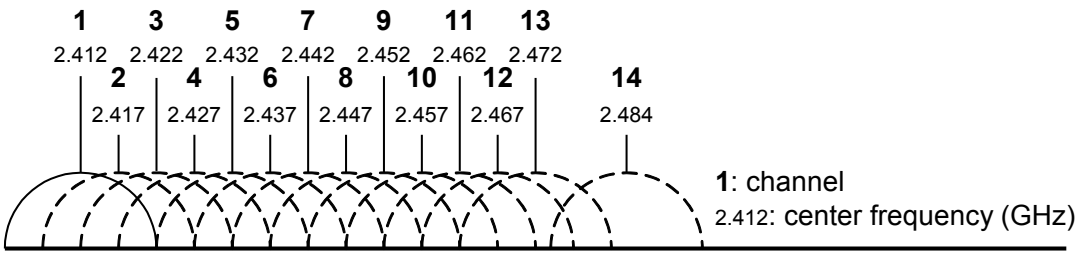
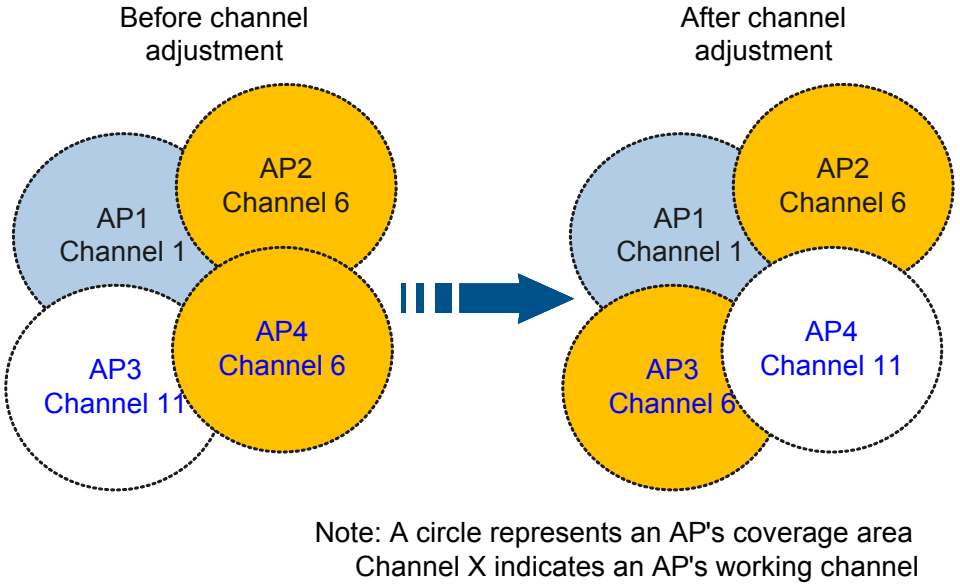


Figure 3-2 shows the channel distribution before and after channel adjustment. Before channel adjustment, both AP2 and AP4 use channel 6. After channel adjustment, AP4 uses channel 11 so that it does not interfere with AP2.

After channel adjustment, each AP is allocated an optimal channel to minimize or avoid adjacent-channel or co-channel interference, ensuring reliable data transmission on the network.

Figure 3-2 Channel adjustment



In addition to optimizing radio performance, channel adjustment can also be used for dynamic frequency selection (DFS). In some regions, radar systems work in the 5 GHz frequency band, which interfere with radio signals of APs working in the 5 GHz frequency band. The DFS function enables APs to automatically switch to other channels when they detect interference on their current working channels.

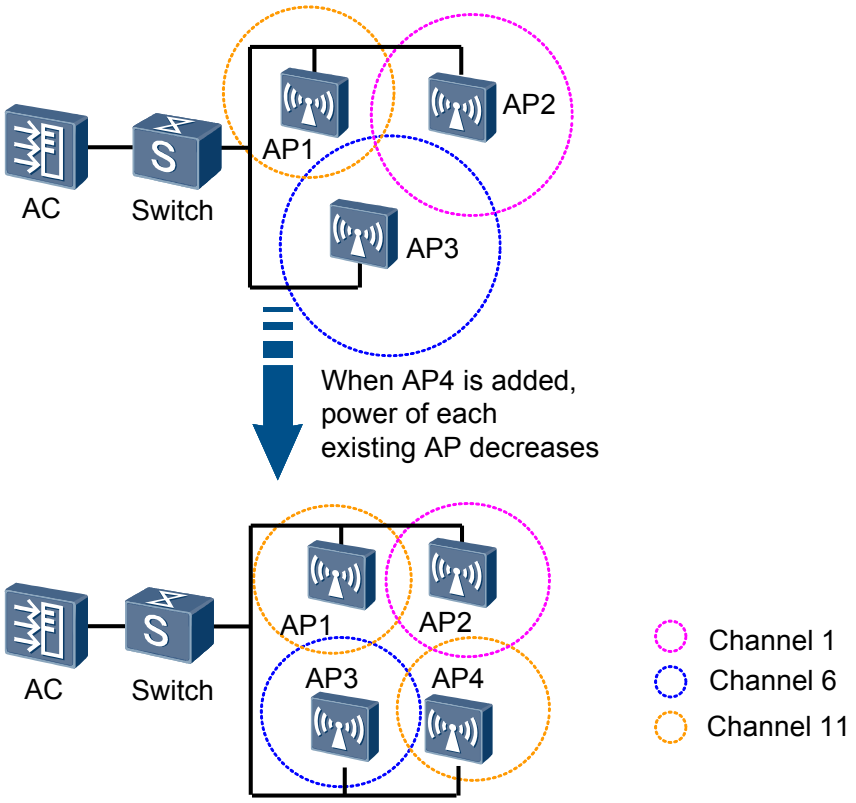
- Power adjustment

  An AP's transmit power determines its radio coverage area. APs with higher power have larger coverage areas. A traditional method to control the radio power is to set the transmit power to the maximum value to maximize the radio coverage area. However, a high transmit power may cause interference to other wireless devices. Therefore, an optimal power is required to balance the coverage area and signal quality.

  The power adjustment function helps dynamically allocate proper power to APs according to the real-time radio environment.

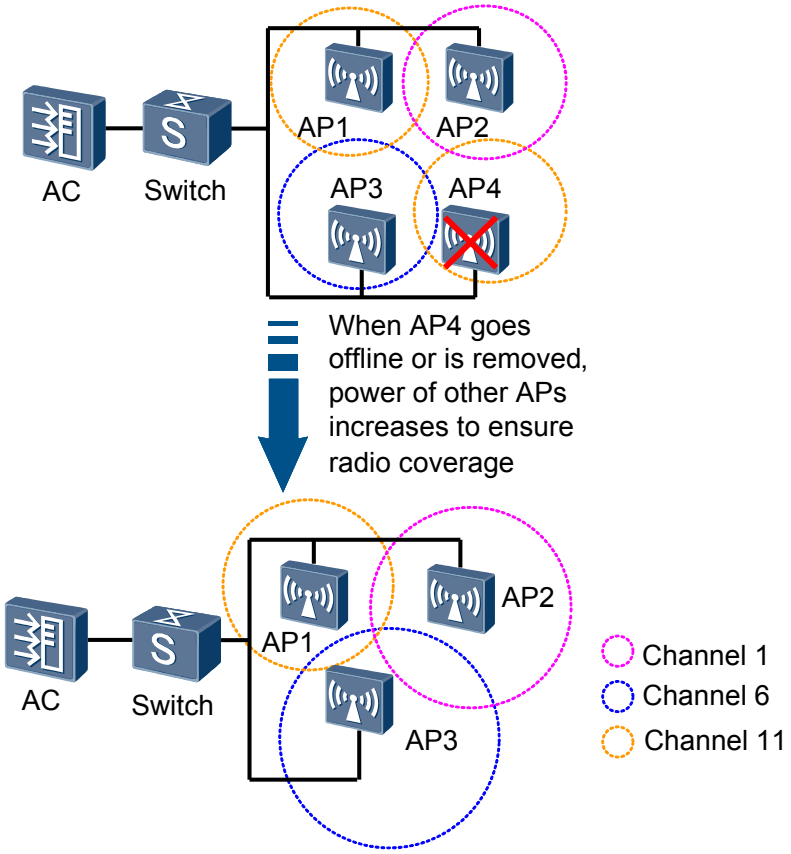
  - When an AP is added to the network, the transmit power of neighboring APs decreases. As shown in **Figure 3-3**, the area of the circle around an AP represents the AP's transmit power and coverage area. When AP4 is added to the network, transmit power of each AP decreases automatically.

Figure 3-3 Transmit power of APs decreases



- When an AP goes offline or fails, power of neighboring APs increases, as shown in **Figure 3-4**.

Figure 3-4 Transmit power of APs increases



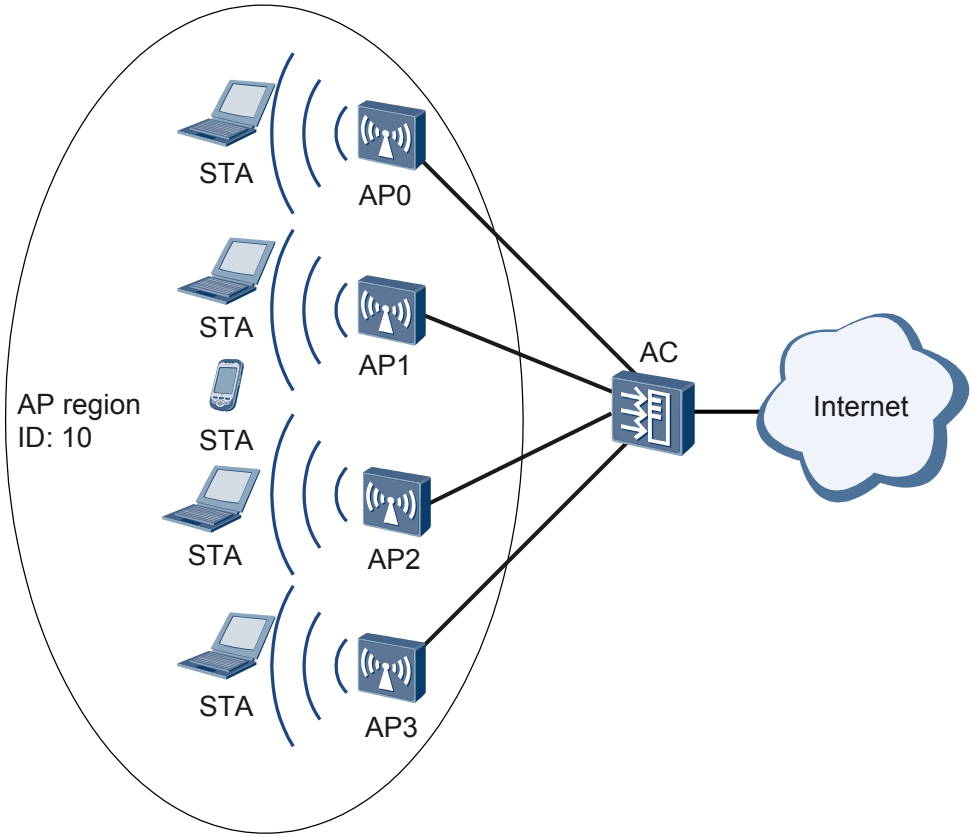
Implementation

An AC supports global radio calibration and partial radio calibration:

- Global radio calibration: takes effect in an AP region. The AC controls channels and transmit power of all APs in the region to achieve best radio performance. Generally, this calibration mode is used on a newly deployed WLAN or a WLAN with a few services.

  On a network shown in **Figure 3-5**, the global radio calibration process is as follows:

Figure 3-5 Implementation of global radio calibration



1. After global radio calibration is enabled, the AC requests the APs to start neighbor probing in the order of AP IDs, starting with AP0.
2. When AP0 receives a probe message from the AC, it listens on Beacon frames on all channels and sends a response message to the AC. After traversing all the channels, AP0 sends the probing result to the AC.
3. When the AC receives the response message from AP0, it sends a probe message to AP1, requesting AP1 to start neighbor probing. When AP1 receives the probe message from the AC, it listens on Beacon frames on all channels and sends a response message to the AC. After traversing all the channels, AP1 sends the probing result to the AC.
4. When the AC receives the response message from AP1, it sends a probe message to AP2, requesting AP2 to start neighbor probing. When AP2 receives the probe message from the AC, it listens on Beacon frames on all channels and sends a response message to the AC. After traversing all the channels, AP2 sends the probing result to the AC.
5. When the AC receives the response message from AP2, it sends a probe message to AP3, requesting AP3 to start neighbor probing. When AP3 receives the probe message from the AC, it listens on Beacon frames on all channels and sends a response message to the AC. After traversing all the channels, AP3 sends the probing result to the AC.
6. After the AC receives probing results of all the APs, it uses the global radio calibration algorithm to allocate channels and power to APs, and sends the results to all the APs.

- Partial radio calibration: The AC dynamically allocates channels and power to specified APs. Generally, this calibration mode is used when new APs are added to the network or the radio environment deteriorates in some areas.

On a network shown in **Figure 3-5**, if AP1 needs radio calibration, the calibration process is as follows:

1. After partial radio calibration is enabled for AP1, the AC sends a probe message to AP1, requesting AP1 to start neighbor probing.
2. AP1 listens on Beacon frames on all channels. After traversing all the channels, AP1 sends the probing result to the AC.
3. The AC uses the partial radio calibration algorithm to allocate a proper channel and power to AP1, and sends the result to AP1.

Background Neighbor Probing

During global or partial radio calibration, an AP needs to listen on Beacon frames on each channel until all channels are probed. The probing process takes a long time and may cause service interruption. If background neighbor probing is enabled, an AP does not need to traverse all channels after receiving a probe message from the AC. Instead, the AP reports the previous probe result to the AC. This reduces risks of service interruption caused by radio calibration.

If background neighbor probing is enabled before radio calibration, an AP determines whether to switch to another channel for neighbor probing every 300s based on the service traffic volume and threshold of user quantity. If the channel switching condition is met (the number of users or traffic on the channel does not exceed the threshold), the AP switches to the new channel. The AP then listens on Beacon frames on the new channel and saves the probing result. After 300 ms, the AP switches back to the original channel.

3.2.2 Load Balancing

Implementation

As shown in **Figure 3-6**, AP1 and AP2 associate with an AC. Four users (STA1 to STA4) associate with AP1, and one user (STA5) associates with AP2. If too many users connect to the Internet through AP1, AP1 will be overloaded, whereas resources on AP2 are not used.

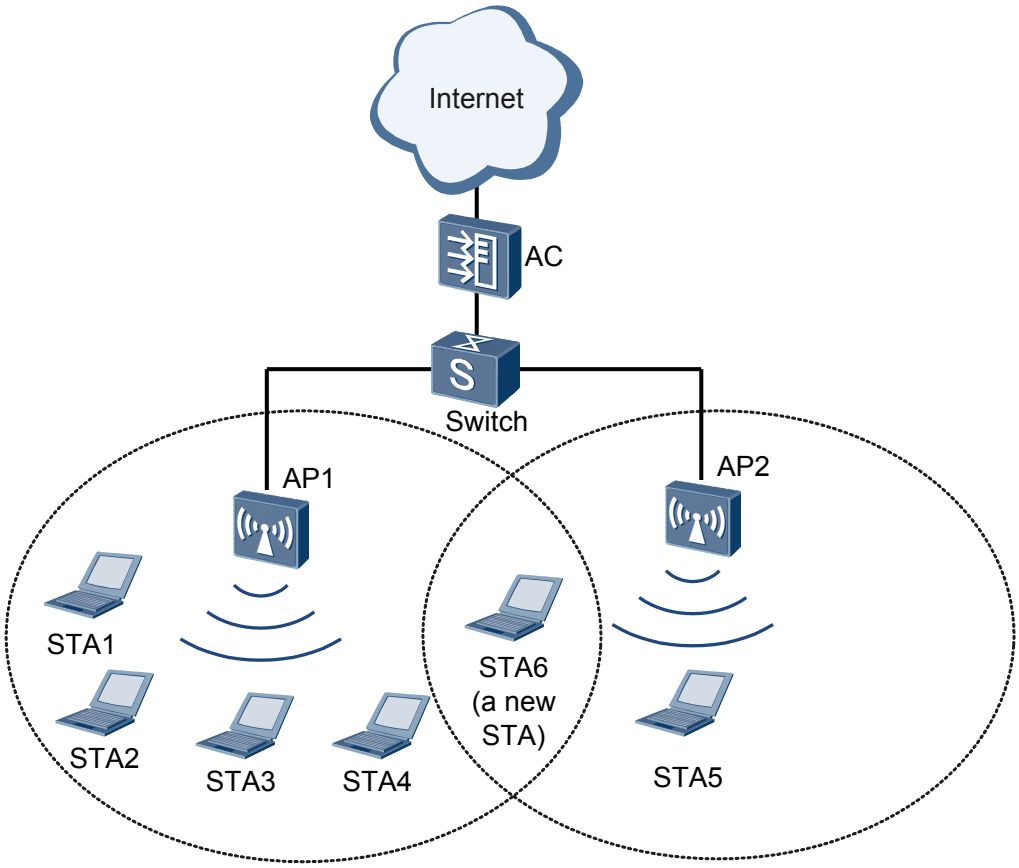
Load balancing can evenly distribute user traffic to different APs to ensure high performance and bandwidth for each STA. The load balancing function applies to wireless networks with high user densities to ensure proper distribution of traffic from STAs.

After load balancing is configured on an AC, the AC uses a load balancing algorithm to determine whether a new STA (STA6 in **Figure 3-6**) can associate with an AP. The load balancing algorithm prevents new STAs from associating with heavily-loaded APs to reduce loads on these APs.

NOTE

Load balancing can be implemented among APs only when the APs are connected to the same AC and all these APs can be discovered by a STA.

Figure 3-6 WLAN load balancing



Load Balancing Mode

Depending on whether a load balancing group needs to be manually created, load balancing is classified in to static and dynamic load balancing:

- Static load balancing: APs providing the same services are manually added to a load balancing group. Each AP periodically reports STA association information to the AC, and the AC distributes user traffic among APs based on received STA association information. When a STA sends an association request, the AP uses a load balancing algorithm to determine whether to accept the association request. Static load balancing can be implemented when the following conditions are met:
  - All APs in a load balancing group work in the same frequency band (2.4 GHz or 5 GHz band).
  - A radio can join only one load balancing group. APs in **Figure 3-6** are single-band APs that support only one frequency band (2.4 GHz or 5 GHz band). If dual-band APs are used, traffic is load balanced among APs working in the same frequency band. That is, a dual-band AP can join two load balancing groups.
  - APs in a load balancing group use different working channels.
  - Each load balancing group supports a maximum of three APs.
- Dynamic load balancing: A STA sends broadcast Probe Request frame to scan available APs. The APs that receive the Probe Request frame all report the STA information to the AC. The AC adds these APs to a load balancing group, and then uses a load balancing

algorithm to determine whether to allow access from the STA. Dynamic load balancing does not limit the number of load balancing members and does not require load balancing members to be manually configured and reside on the same frequency band. Therefore, dynamic load balancing can ensure bandwidth of each STA.

Depending on the load balancing algorithm used, load balancing is classified into traffic-based load balancing and session-based load balancing:

- Traffic-based load balancing: Traffic is load balanced based on the difference between the traffic volume on different radios. The traffic-based load balancing algorithm is as follows:

  The AC calculates the load percentage of each radio in a load balancing group using the formula:

  Load percentage of a radio = (Traffic rate of the radio/Maximum rate of the radio) x 100%

  The AC compares load percentages of all radios in the load balancing group and obtains the smallest load percentage value. When a STA requests to associate with an AP radio, the AC calculates the difference between the radio's load percentage and the smallest load percentage value and compares the load difference with the threshold (configured using a command). If the load difference is smaller than the threshold, the AC allows the STA to associate with the radio. If not, the AC rejects the association request of the STA. If the STA continues sending association requests to this AP, the AC allows the STA to associate with the AP when the number of association requests sent by the STA exceeds the maximum number configured on the AC.

- Session-based load balancing: Traffic is load balanced based on differences between STA quantities on different radios. The session-based load balancing algorithm is as follows:

  The AC calculates the load percentage of each radio in a load balancing group using the formula:

  Load percentage of a radio = (Number of associated STAs on the radio/Maximum number of STAs allowed on the radio) x 100%

  The AC compares load percentages of all radios in the load balancing group and obtains the smallest load percentage value. When a STA requests to associate with an AP radio, the AC calculates the difference between the radio's load percentage and the smallest load percentage value and compares the load difference with the threshold (configured using a command). If the load difference is smaller than the threshold, the AC allows the STA to associate with the radio. If not, the AC rejects the association request of the STA. If the STA continues sending association requests to this AP, the AC allows the STA to associate with the AP when the number of association requests sent by the STA exceeds the maximum number configured on the AC.

The following explains the session-based load balancing algorithm in static load balancing mode.

As shown in **Figure 3-6**, four STAs (STA1 to STA4) has associated with AP1 and only STA5 has associated with AP2. Assume that AP1 and AP2 each allow a maximum of 10 users and the load difference threshold is set to 5%. Now, STA6 requests to associate with AP1.

According to the load percentage calculation formula, the load percentage of AP1's radio is 40% (4/10 x 100% = 40%), and the load percentage of AP2's radio is 10% (1/10 x 100% = 10%). Therefore, the smallest load percentage value is 10%. When STA6 associates with AP1, the load percentage of AP1 will reach 50% (5/10 x 100% = 50%). The difference between this load percentage and the smallest value is 40% (50% - 10% = 40%), larger than the load difference threshold (5%). Therefore, the AC determines that traffic is not evenly distributed between the two APs and prevents STA6 from associating with AP1.

3.2.3 5G-Prior Access

When an AP and STA support both 5 GHz and 2.4 GHz frequency bands, the AP can request the STA to associate with the 5 GHz radio first.

Most STAs support both 5 GHz and 2.4 GHz frequency bands and they usually associate with the 2.4 GHz radio by default when connecting to the Internet. To connect to the 5 GHz radio, users must manually select the 5 GHz radio. When the 2.4 GHz frequency band has many users or severe interference, the 5 GHz frequency band can provide better access service for wireless users. The 5G-prior access function enable STAs to preferentially associate with the 5 GHz radio.

NOTE

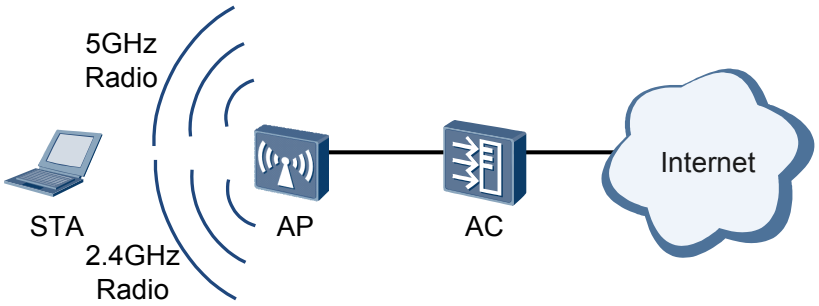
To implement the 5G-prior access function, an AP must have the same SSID and security policy on the 5 GHz and 2.4 GHz radios.

5G-prior access is implemented as follows:

As shown in **Figure 3-7**, when the AP receives a Probe Request frame from the STA, it checks the radio receiving the Probe Request frame. If the Probe Request frame is received by the 2.4 GHz radio, the AP does not return a Probe Response frame. If the Probe Request frame is received by the 5 GHz, the AP returns a Probe Response frame. Then the STA associates with the 5 GHz radio.

If only the 2.4 GHz radio receives 25 Probe Request frames continuously but the 5 GHz radio does not receive any Probe Request frame, the AP returns a Probe Response frame through the 2.4 GHz radio. Then the STA associates with the 2.4 GHz radio.

Figure 3-7 5G-prior access



3.2.4 Spectrum Analysis

Overview

Wireless interference includes WLAN interference and non-WLAN interference. WLAN interference can be detected using interference detection technologies. Non-WLAN interference can be detected using spectrum analysis technologies.

In spectrum analysis, the spectrum analysis server analyzes the characteristics of collected wireless signals to identify and locate non-WLAN (non-Wi-Fi) devices, eliminating the impact of interference on WLANs.

Implementation

Spectrum analysis is implemented as follows:

1. The AP scans and samples the spectrum. An AP scans and samples the spectrum only in monitoring or hybrid mode.
   - When an AP works in hybrid mode, the AP can monitor wireless devices while transmitting data. The AP not only collects spectrum data of working channels but also periodically switches to non-working channels to collect data, and generates fast fourier transform (FFT) data.
   - When an AP works in monitoring mode, the AP can monitor wireless devices but cannot transmit data of WLAN users. The AP periodically collects spectrum data of each channel to generate FFT data.
2. The AP sends the sampled spectrum data to the AC.

   The AP will collect a large amount of data within a sample interval, so it needs to fragment the data into multiple packets before sending the data. The AP adds the start identifier and total number of packets to the first sent packet, adds the end identifier to the last sent packet, encapsulates the packets in UDP packets, and sends the packets to the AC.
3. The AC receives and cache the spectrum data sent from the AP.

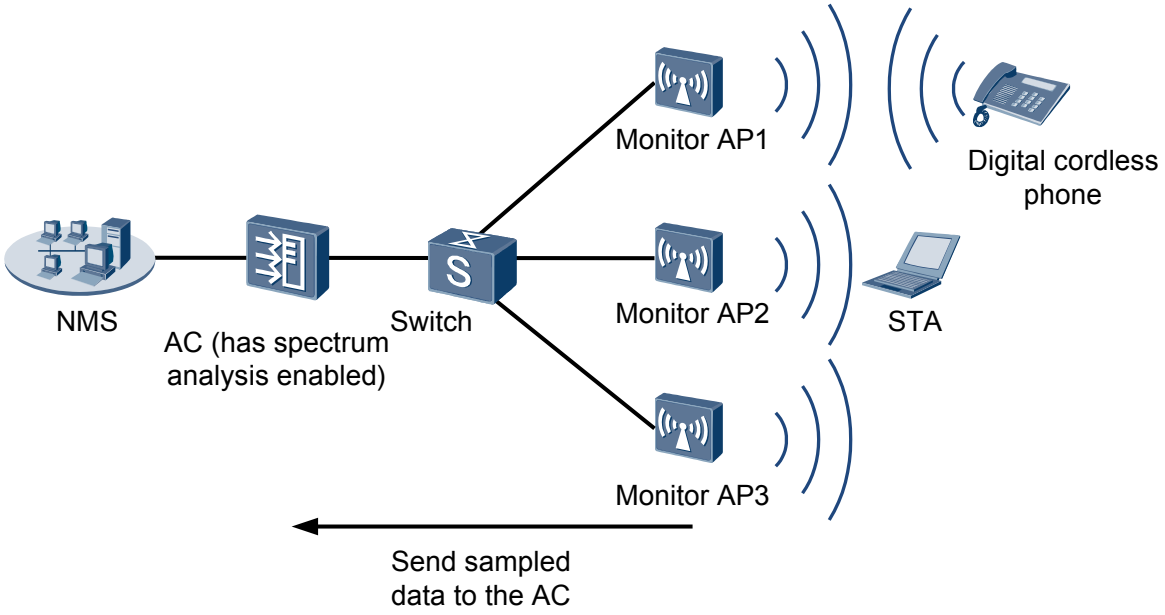
   The data sampled by the AP needs to be fragmented into about 80 packets for UDP transmission. When receiving the first packet from the AP, the AC starts the timer and caches all the spectrum data collected before the timer times out. If the AC receives the packet carrying the end identifier before the timer times out, the AC sends all the cached packets to the spectrum analysis module for spectrum analysis. Otherwise, the AC discards the sampled data.
4. The AC's spectrum analysis module analyzes the spectrum of sampling points.

   The spectrum analysis module identifies the pulse and extracts the characteristics of sampling points to identify terminal devices. The module can identify baby monitors, bluetooth devices, digital cordless phones (at 2.4 GHz frequency band only), wireless audio transmitters (at both the 2.4 GHz and 5 GHz frequency bands), and microwaves. The AP adds the identified devices into the unauthorized device list. If the type of an identified device is not specified in the unauthorized device list, the AP reports an alarm. If the type of the identified device is already in the updated list, the AP does not report an alarm. If the device ages or manually deleted, the AP reports an alarm indicating that the device is deleted.

Typical Applications

On the 2.4 GHz WLAN shown in **Figure 3-8**, user access experience is still unsatisfactory after radio calibration is performed. For example, packet loss occurs when users ping a website address. To improve user access experience, configure one or multiple APs on the WLAN to work in monitoring mode to detect whether non-WLAN interference exists around the WLAN.

Figure 3-8 Spectrum analysis networking



3.3 References

The following table lists the reference for this feature.

Document	Description	Remarks
IEEE 802.11k	Radio Resource Measurement of Wireless LANs	-

4 WLAN Reliability

About This Chapter

4.1 Introduction to WLAN Reliability
4.2 Principles
4.3 Applications
4.4 References

4.1 Introduction to WLAN Reliability

As WLAN technologies develop, a lot of users access the Internet through the WLAN. Reliability is a major problem to be solved in WLAN transmission. A reliable WLAN can effectively reduce impact of network faults and service interruption.

4.2 Principles

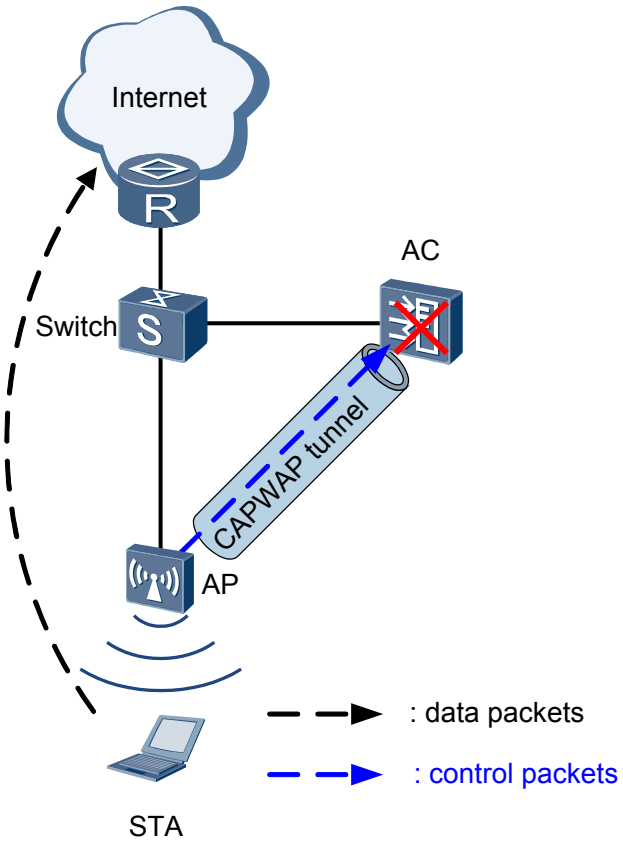
4.2.1 Non-Stop AP Operation After CAPWAP Link Disconnection

In the direct forwarding scenario that uses the AC+Fit AP architecture, the AP and AC must establish a CAWAP tunnel for control packet forwarding before a STA connects to the Internet through WLAN. When the CAPWAP tunnel is faulty, the AP cannot forward data packets, online users on the AP are forcibly disconnected from the AP, and new users cannot connect to the AP. These problems affect user experience.

- Service holding upon CAPWAP link disconnection

  After the service holding function is enabled, the AP can still forward data packets when the CAPWAP tunnel is faulty, ensuring nonstop data service transmission in direct forwarding mode. This function reduces loss for users and improves service reliability.

Figure 4-1 Service holding upon CAPWAP link disconnection



- User access permission after CAPWAP link disconnection

  The service holding function takes effect only for online users but not for offline users. Offline users are not allowed to go online when the CAPWAP link is broken.

  When the function that allows user access after CAPWAP link disconnection is enabled, the AP stills allow offline users to go online and access all network resources that are available before the CAPWAP link is broken. After the broken CAPWAP link is restored, the AP forces all the STAs that have gone online during CAPWAP link disconnection to go offline. The AP then automatically re-associates with the STAs and reports information about the STAs through logs.

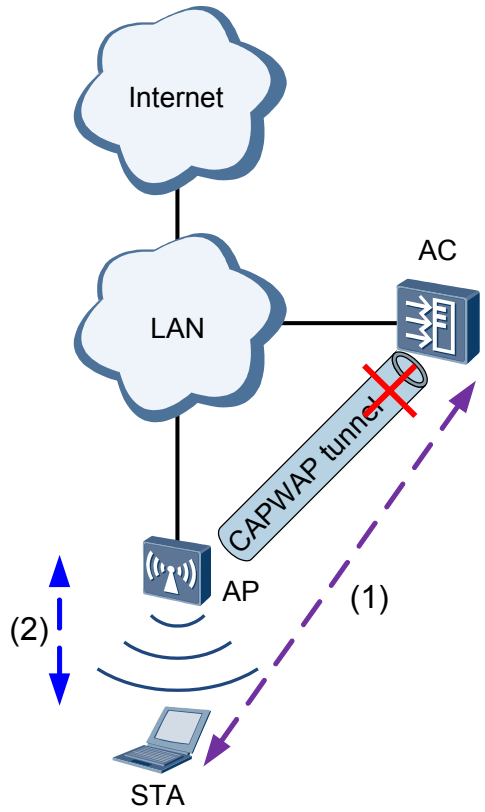
  NOTE

  This function takes effect only when the WLAN uses open system authentication, pre-shared key authentication, or WPA/WPA2–PSK authentication.

  This function allows all the users that enter the correct key to go online. The STA whitelist and blacklist configured on the AC do not take effect after the CAPWAP link is broken.

  As shown in **Figure 4-2**, when the function that allows user access after CAPWAP link disconnection is disabled, the STA association and key negotiation are performed between the AC and STA. After this function is enabled, the STA authentication, association, and key negotiation are performed between the AP and STA.

Figure 4-2 User access permission after CAPWAP link disconnection



(1) Authentication packet exchange before user access permission after CAPWAP link disconnection is disabled

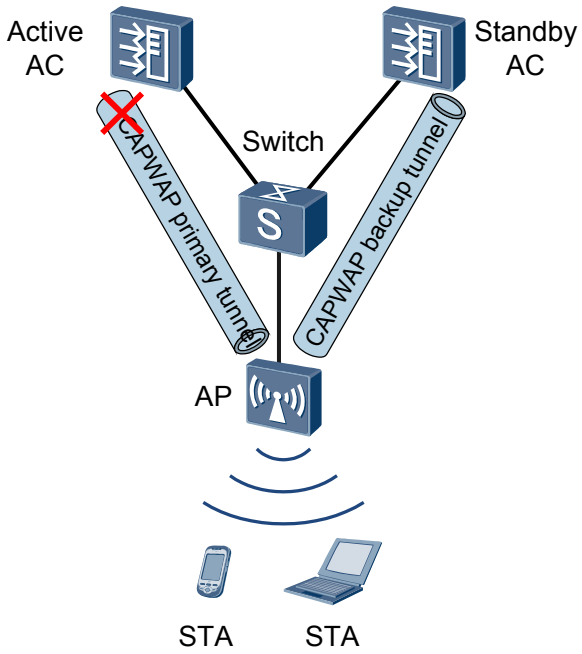
(2) Authentication packet exchange before user access permission after CAPWAP link disconnection is enabled

4.2.2 Dual-Link Backup

In the AC + Fit AP networking, the AC manages and controls WLAN services of users. An AC may control hundreds of APs and thousands of STAs; therefore, the AC must be highly reliable. If the AC is faulty, the services of all users connected to the AC are interrupted.

As shown in **Figure 4-3**, an active AC and a standby AC are deployed on the WLAN. The AP establishes tunnels with the two ACs (**CAPWAP Tunnel Setup**), and periodically exchanges CAPWAP packets with ACs to monitor link status. The active AC controls access of STAs. If the AP detects a fault on the link between AP and active AC, the AP requests the standby AC to trigger an **Active/Standby Switchover**. The standby AC then becomes the active AC to control access of STAs. After the original active AC is restored, the AP requests the active and standby ACs to perform **Revertive Switchover**. The restored AC becomes the active AC again.

Figure 4-3 Dual-link backup networking diagram



CAPWAP Tunnel Setup

1. Setting up the first tunnel

   The procedure for setting up the first tunnel is the same as the procedure for setting up a CAPWAP tunnel, except that the active AC needs to be selected in Discovery phase. Only the Discovery phase is described in this section. For description of other phases, see "CAPWAP Tunnel Establishment" in **1.2.4 AP Login**.

   a. After the dual-link backup function is enabled in Discovery phase, the AP sends a Discovery Request message in unicast or broadcast mode:

      - If the IP addresses of active and standby ACs have been allocated in static, DHCP, or DNS mode, the AP sends the Discovery Request message in unicast mode to request connections with the ACs.
      - If no IP addresses are allocated to ACs or there is not response to the unicast packet, the AP sends another Discovery Request message in broadcast mode to discover the ACs that can be associated with the AP.

   b. As long as the ACs are working properly, they will return Discovery Response messages to the AP. The Discovery Response messages contain the dual-link backup flag, priorities, load, and IP addresses of the ACs.

   c. After receiving the Discovery Response message, the AP selects an active AC based on AC priorities, loads, and IP addresses and sets up a CAPWAP primary tunnel with the active AC. The AP selects the active AC in the following sequence:

      a. Compare AC priorities, and select the AC with the smaller priority value as the active AC.

      b. When the AC priorities are the same, compare the loads, that is, the number of APs and STAs. Select the AC connecting to fewer APs and STAs as the active AC.

      c. When the loads are the same, compare the ACs' IP addresses, and select the AC with the smaller IP address as the active AC.

2. Setting up the second tunnel with the other AC

   To prevent repeated service configuration delivery, the AP starts to set up the second tunnel only after the configuration of the first tunnel is complete.

   a. The AP sends a Discovery Request message to the other AC in unicast mode.
   b. The AC returns a Discovery Response message containing the dual-link backup flag, load, and priority to the AP.
   c. The AP knows that the dual-link backup function is enabled after receiving the Discovery Response message, and saves the priority of the AC.

      NOTE

      If the priority of this AC is higher than the priority of the other AC, the AP performs an active/standby switchover only after the tunnel is set up.

   d. The AP sends a Join Request message, notifying the AC that the configurations have been delivered. After receiving the Join Request message, the AC sets up a CAPWAP tunnel with the AP but does not deliver configurations to the AP.
   e. After the second tunnel is set up, the AP selects the active and standby ACs again based on the tunnel priorities.

Active/Standby Switchover

After setting up tunnels with the active and standby ACs, the AP sends Echo messages to monitor tunnel status. The Echo messages contain the active/standby status of the tunnels. When the AP detects that the primary tunnel fails, it sends an Echo Request message with the active flag to the standby AC. After receiving the Echo Request message, the standby AC becomes the active AC, and the AP transfers STA data to this AC.

Revertive Switchover

The AP periodically sends Discovery Request messages to check whether the original primary tunnel recovers. If the original primary tunnel recovers, the AP switches STA data back to this tunnel after a delay because this tunnel has a higher priority than the other one. To prevent frequent switchovers caused by network flapping, the AP requests ACs to perform revertive switchover after 20 Echo intervals, and then sends STA data to the new active AC.

4.2.3 AC Hot Standby

In dual-link backup, an AP periodically sends Echo packets to the active and standby ACs to monitor the link status. If the AP does not receive any response from the AC after the Echo packets are sent for the specified number of times, the AP triggers an active/standby switchover. When the AP determines whether to trigger an active/standby switchover, services are interrupted.

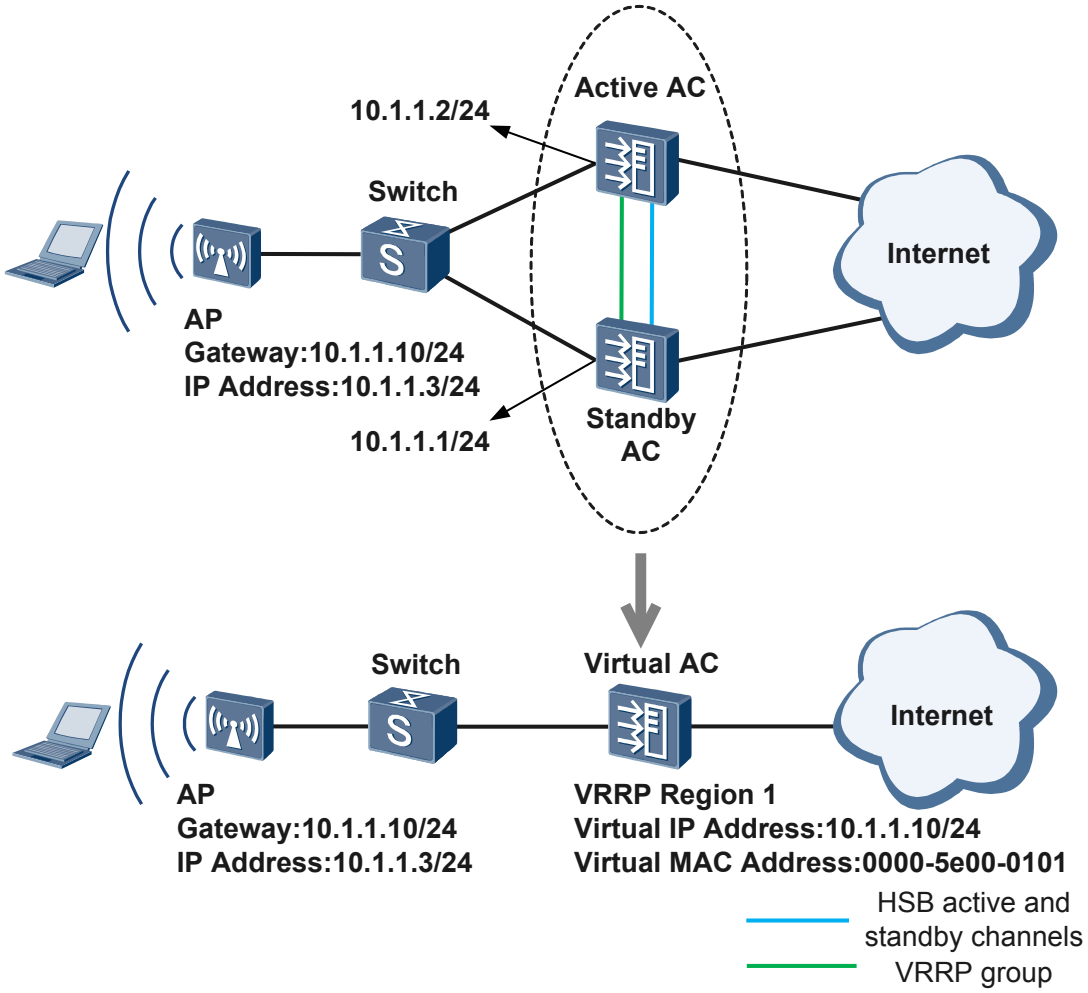
To prevent service interruption in dual-link backup, the AC hot standby mechanism is used to ensure that services are seamlessly switched to the standby AC when the active AC fails. This mechanism ensures non-stop enterprise service transmission and improves reliability.

AC hot standby can be implemented in two modes:

- Hot standby backup (HSB)+Virtual Router Redundancy Protocol (VRRP): An AP can obtain only one AC's IP address. This IP address is the virtual IP address of the active and standby ACs in a VRRP group. The active and standby ACs are elected among the ACs in the VRRP group based on the AC priority. The active AC manages and controls all APs

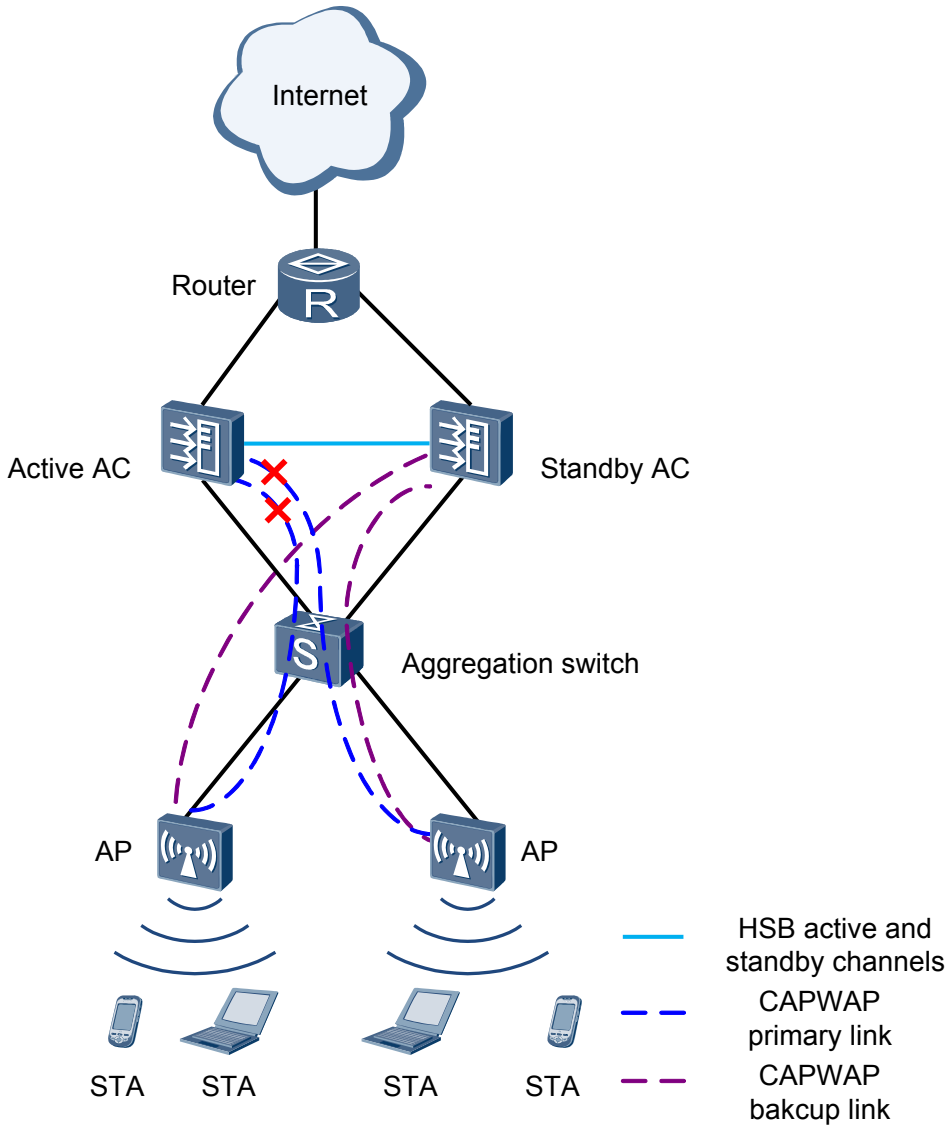
and STAs and periodically sends status information and information to be backed up to the standby AC through the HSB function in scheduled and real-time backup modes. The information to be backed up includes AC entries, CAPWAP link information, and user information. When a fault occurs on the active AC, the standby AC can fast detect the fault on the active AC through the CAPWAP heartbeat mechanism and become the new active AC in a timely manner. This function ensures nonstop user services.

Figure 4-4 HSB+VRRP networking



- HSB+dual-link backup: An AP establishes CAPWAP tunnels with both the active and standby ACs. The two ACs back up user information through the HSB function. When the active AC becomes faulty, the AP detects that the active AC fails and switches the standby CAPWAP tunnel as the new active CAPWAP tunnel.

Figure 4-5 HSB+dual-link backup networking

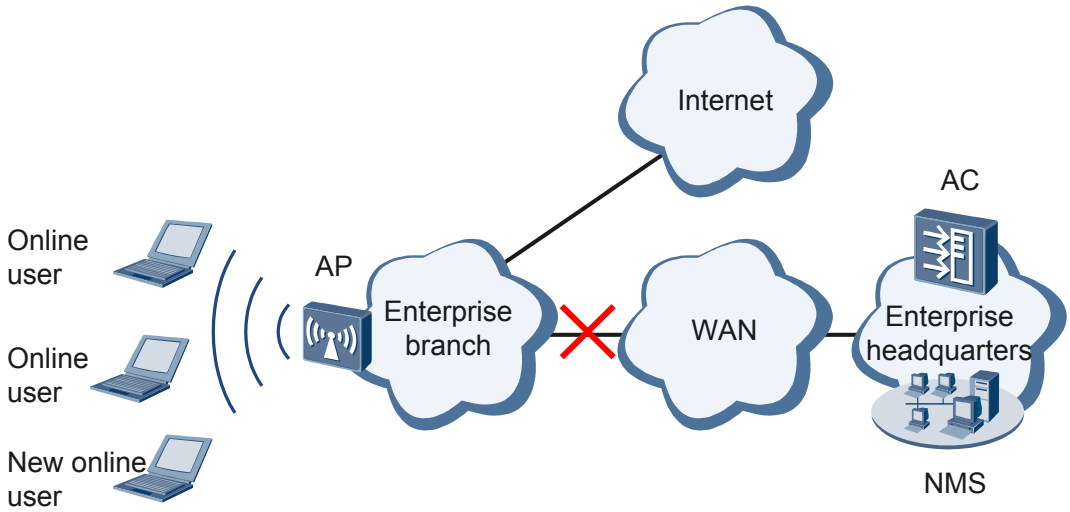


4.3 Applications

4.3.1 Application of Non-Stop AP Operation After CAPWAP Link Disconnection

As shown in **Figure 4-6**, to reduce management and maintenance costs, some small- and medium-sized enterprises deploy the AC at the headquarters to manage the APs and STAs in branches. In the direct forwarding scenario, after the CAPWAP link between the AP and AC is broken, online branch users can access local network resources (such as the local servers), and new branch users can still access the WLAN to obtain network resources.

Figure 4-6 Non-stop AP operation after CAPWAP link disconnection

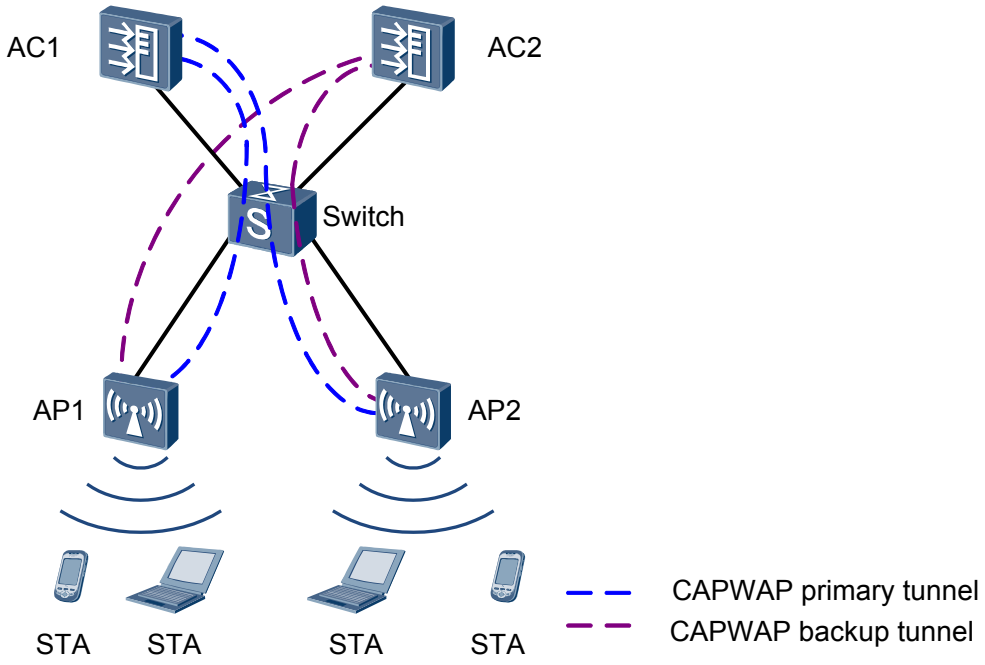


4.3.2 Application of Dual-Link Backup

1+1 Dual-Link Backup

As shown in **Figure 4-7**, AC1 and AC2 provide dual links for STAs. AC1 is the active device, serving AP1 and AP2. AC2 is the standby device. When the APs detect that AC1 fails, the CAPWAP tunnels between APs and AC2 become the active tunnels, and AC2 becomes the active AC. After AC1 recovers, it becomes the active AC or still functions as the standby AC depending on the configuration.

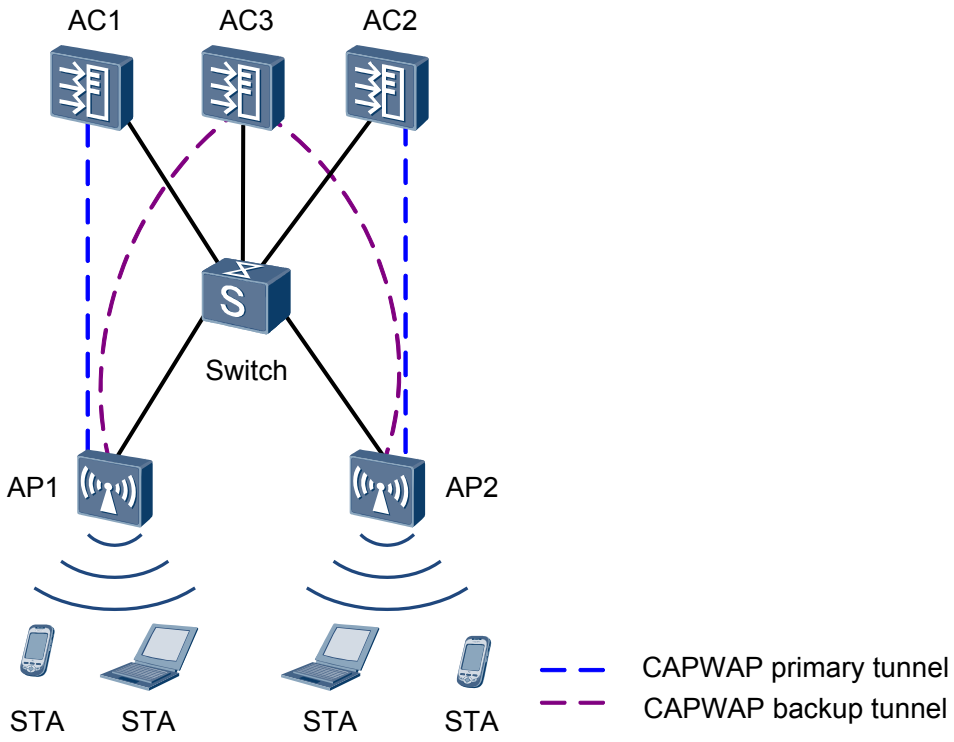
Figure 4-7 1+1 dual-link backup networking diagram



N+1 Link Backup

As shown in **Figure 4-8**, AC1 functions as the active AC for AP1, AC2 functions as the active AC for AP2, and AC3 functions as the standby AC for AP1 and AP2. When AC1 or AC2 is faulty, the data from AP1 or AP2 is switched to AC3, ensuring nonstop service transmission.

Figure 4-8 N+1 link backup networking diagram



4.3.3 Application of AC Hot Standby

On a wireless access network, an AC can manage several hundred APs. If the AC becomes faulty, services of all the APs that associate with the AC are interrupted. To reduce impact of AC faults, a traditional backup solution deploys two devices on an access node for backup. An AC on a wireless network usually run Dynamic Host Configuration Protocol (DHCP), network admission control (NAC), and wireless local area network (WLAN) services, which require real-time information backup from the active device to the standby device. For example, the active DHCP device must synchronize user status information to the standby DHCP device in real time. Otherwise, services will be interrupted after link switching.

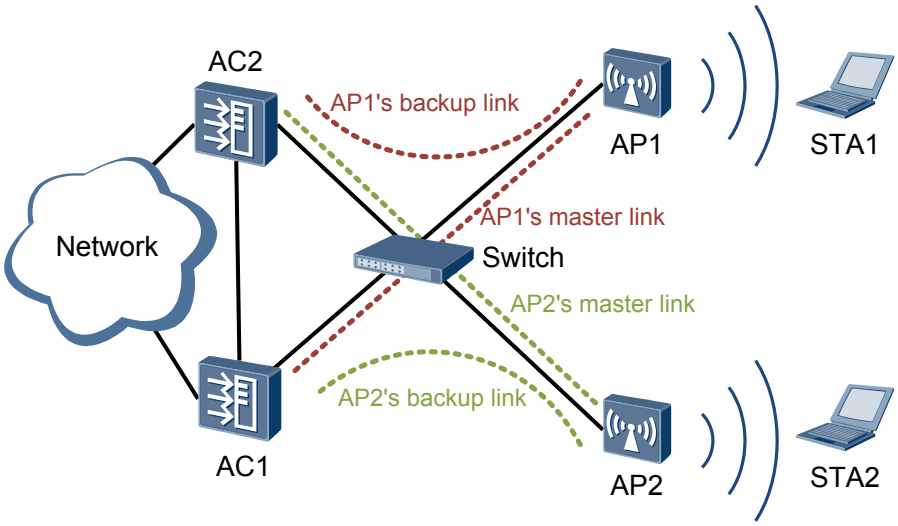
The AC hot standby function can solve this problem. This function has two modes: HSB+VRRP and HSB+dual-link backup. HSB supports batch backup and real-time backup between the two access devices. When the active device fails, service traffic is immediately switched to the standby device without interrupting services. This improves connection availability. Dual-link backup or VRRP can fast detect whether the active AC is faulty so that the standby AC can become the new active AC in a timely manner. This function ensures user service continuity.

HSB+Dual-Link Backup

In **Figure 4-9**, an enterprise deploys two ACs: AC1 (active AC) and AC2 (standby AC). AP1 associates with AC1, and AP2 associates with AC2. NAC and WLAN services are deployed on AC1 and AC2. AC1 and AC2 are bound to the same HSB tunnel.

Load balancing can be implemented on AC1 and AC2 to fully use network resources. For AP1, AC1 is the active device and AC2 is the standby device. All service traffic of AP1 is forwarded by AC1. For AP2, AC2 is the active device and AC1 is the standby device. All service traffic of AP2 is forwarded by AC2. Traffic of AP1 and AP2 is load balanced between the two ACs, improving link efficiency.

Figure 4-9 HSB+dual-link backup networking

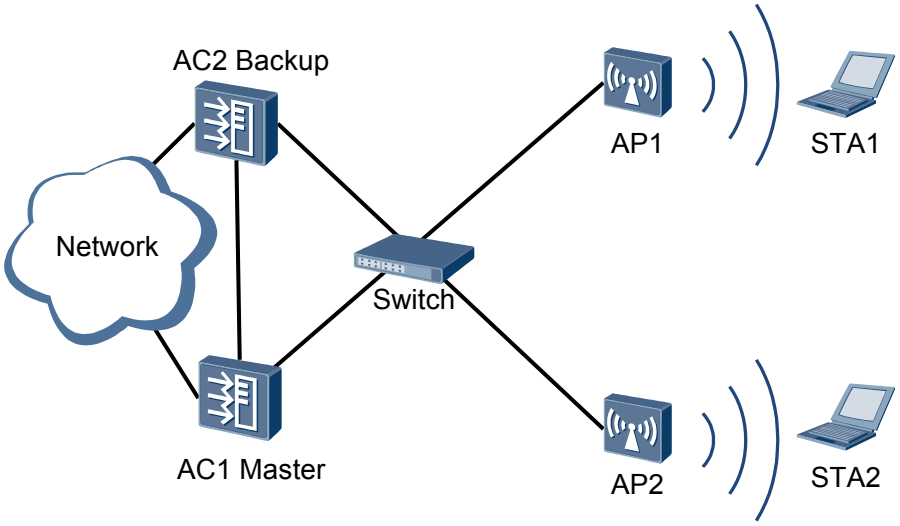


HSB+VRRP

In **Figure 4-10**, an enterprise deploys two ACs: AC1 (active AC) and AC2 (standby AC). AP1 associates with AC1, and AP2 associates with AC2. DHCP, NAC, and WLAN services are deployed on AC1 and AC2. AC1 and AC2 are bound to an HSB group that works in active/standby mode.

When AC1 fails, AC2 immediately takes over the DHCP, NAC, and WLAN services because it has backed up all the required information from AC1. Services are not interrupted after the link switching.

Figure 4-10 HSB+VRRP networking



4.4 References

None

5 WLAN Roaming

About This Chapter

5.1 Introduction to WLAN Roaming

5.2 Principles

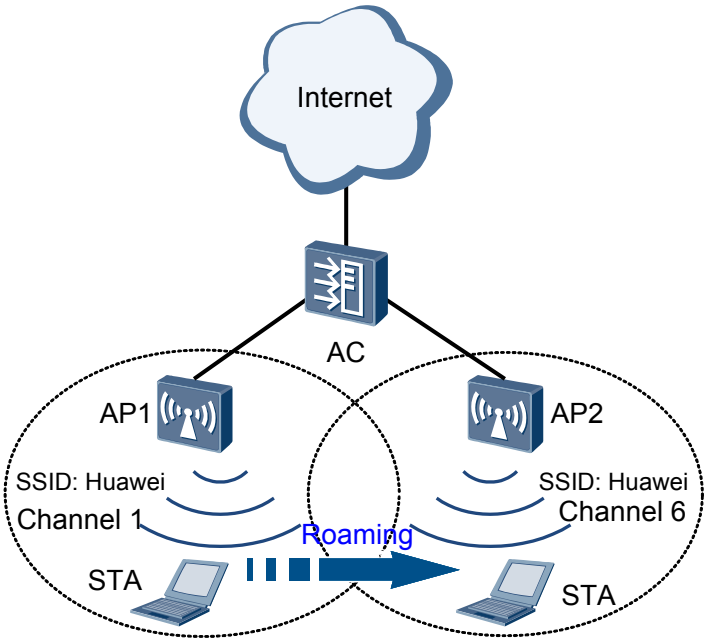
5.3 References

5.1 Introduction to WLAN Roaming

Definition

WLAN roaming allows a STA to move from an AP to another AP in the same ESS on a WLAN network with nonstop service transmission. In **Figure 5-1**, the STA moves from AP1 to AP2.

Figure 5-1 WLAN roaming networking



WLAN roaming includes roaming between APs in the same service VLAN and roaming between APs in different service VLANs:

- Roaming between APs in the same service VLAN: APs before and after STA roaming belong to the same service VLAN.
- Roaming between APs in different service VLANs: APs before and after STA roaming belong to different service VLANs. To prevent services of a user from being interrupted during WLAN roaming, ensure that the service VLAN of the user remains unchanged after the user roams between two APs.

WLAN roaming is classified into fast roaming and non-fast roaming based on the security policy used by STAs. As shown in **Table 5-1**, fast roaming can be implemented only when the security policy is WPA2-802.1x and STAs support fast roaming. When the security policy is not WPA2-802.1x, non-fast roaming is implemented regardless of whether STAs support fast roaming. When the security policy is WPA2-802.1x but STAs do not support fast roaming, non-fast roaming is implemented.

Table 5-1 Fast roaming and non-fast roaming

Security Policy	Whether Access Authentication Is Required Again	Whether STAs Support Fast Roaming	Roaming Mode
WEP open system authentication	No	N/A	Non-fast roaming
WEP shared key authentication	No	N/A	Non-fast roaming
WPA/WPA2-PSK	Yes	N/A	Non-fast roaming
WPA-802.1x	Yes	N/A	Non-fast roaming
WPA2-802.1x	Yes	No	Non-fast roaming
WPA2-802.1x	No	Yes	Fast roaming

Purpose

The biggest advantage of WLAN networks is that a STA can move within a WLAN network regardless of physical media locations. WLAN roaming ensures that a STA moves within a WLAN network without interrupting services. An ESS includes multiple APs. When a STA moves from an AP to another AP, WLAN roaming ensures seamless transition of STA services between APs.

WLAN roaming has the following advantages:

- Prevents packet loss or service interruption caused by long-term authentication.

  If a STA needs to be authenticated before accessing the Internet, the authentication process (for example, 802.1x authentication) may take a long period of time. Fast roaming prevents STA re-authentication, ensuring nonstop user service transmission.
- Ensures that users' IP addresses remain unchanged.

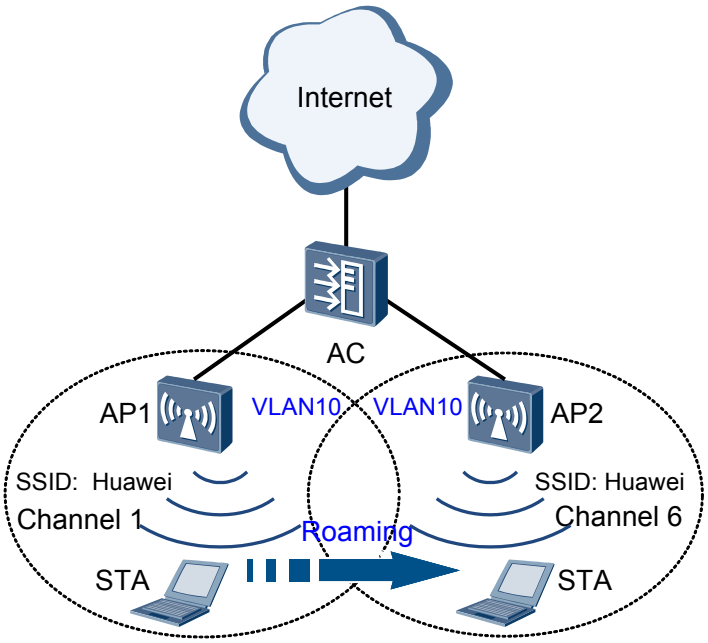
  Application protocol packets are transmitted using IP addresses and TCP/UDP connections. STAs' IP addresses must remain unchanged after WLAN roaming so that the TCP/UDP connections established for the STAs are not interrupted.

5.2 Principles

5.2.1 Roaming Between APs in the Same Service VLAN

Roaming between APs in the same service VLAN allows a STA to move between two APs that connect to the same AC and belong to the same service VLAN without service interruption, as shown in **Figure 5-2**.

Figure 5-2 Roaming between APs in the same service VLAN



Roaming between APs in the same service VLAN is classified into fast roaming and non-fast roaming.

Non-Fast Roaming

Non-fast roaming technology is used when a STA uses a non-WPA2-802.1x security policy. If a STA uses WPA2-802.1x but does not support fast roaming, the STA still needs to complete 802.1x authentication before roaming between two APs.

NOTE

STA needs to roam between two APs, the APs must have the same SSID (for example, the SSIDs in **Figure 5-2** are Huawei) and security policy profile.

In **Figure 5-2**, the STA accesses the Internet through AP1. The STA needs to roam from AP1 to AP2, and the STA roaming process is as follows:

1. The STA sends a Probe Request frame on each channel. After receiving the Probe Request frame, APs send Probe Response frames to the STA. For example, after AP2 receives the Probe Request frame on channel 6 (a channel used by AP2), AP2 sends a Probe Response frame on channel 6 to the STA. When the STA receives Probe Response frames from APs, the STA selects an AP to associate with according to the signal strength and quality. Assume that the STA selects AP2 to associate with as shown in **Figure 5-2**.
2. The STA sends a Re-authentication Request packet on channel 6 to AP2. After the STA is authenticated by AP2, AP2 sends a Re-authentication Response packet to the STA.
3. The STA sends a Re-association Request packet to AP2, which then sends the packet to the AC. The AC sends a Re-association Response packet, allowing the STA to re-associate with AP2.
4. The STA re-associates with AP2 and then disassociates from AP1. The STA sends a Disassociation frame to AP1 on channel 1 (a channel used by AP1) to disassociate from AP1.

- If the STA uses the WEP security policy, the STA roaming process is complete.
- If the STA uses the WPA/WPA2-PSK security policy, the STA needs to perform access authentication and key negotiation again. For details about key negotiation, see **Key Negotiation** in **2.3.1.2 WPA/WPA2**.
- If the STA uses the WPA/WPA2-802.1x security policy, the STA needs to perform access authentication and key negotiation again. For details, see **2.3.1.2 WPA/WPA2**.

Fast Roaming

The roaming switchover time is a key factor that affects WLAN service experience during roaming. When a user uses the WEP or WPA/WPA2-PSK security policy, the roaming switchover time is less than 100 ms, so the user does not detect service interruption during roaming. When the user uses the WPA2-802.1x security policy, the roaming switchover time is more than 100 ms because the user needs to perform 802.1x authentication and key negotiation again. The user then detects service interruption during roaming.

When the user uses the WPA2-802.1x security policy and supports fast roaming, the user does not need to perform 802.1x authentication again during roaming and only needs to perform key negotiation. In this case, fast roaming reduces the roaming delay and improves the WLAN service experience.

Fast roaming is implemented using pairwise master key (PMK) caching. In **Figure 5-2**, the fast roaming process is as follows:

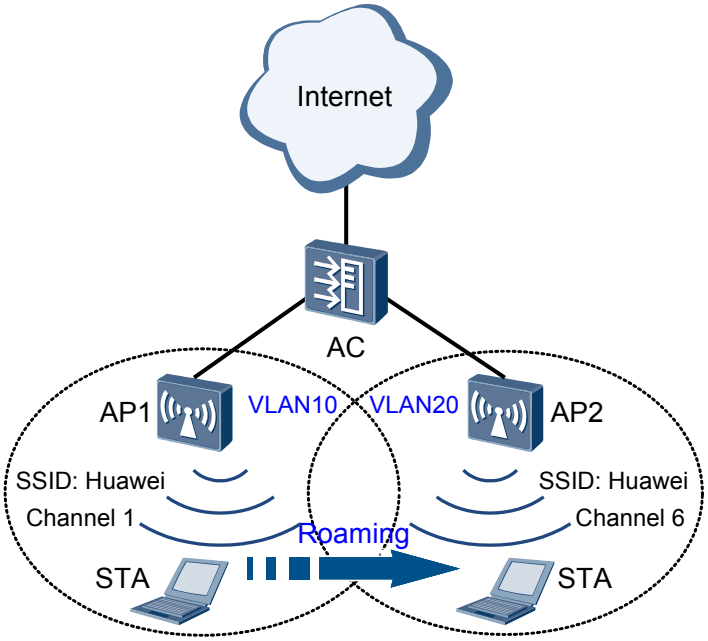
1. The STA accesses the Internet through AP1 for the first time. When the STA is authenticated by the AC and a PMK is generated, the STA and AC save the PMK information. Each PMK has a PMK-ID, which is calculated based on the PMK, SSID, STA MAC address, and BSSID.
2. During roaming, the STA sends AP2 a Re-association Request packet that carries the PMK-ID.
3. AP2 receives the Re-association Request packet and then notifies the AC that the STA needs to roam from AP1 to AP2.
4. The AC searches the PMK caching table for the PMK of the STA according to the PMK-ID carried in the Re-association Request packet. If the AC finds a matching PMK, the AC considers that 802.1x authentication has been performed on the STA and uses the cached PMK for key negotiation.

5.2.2 Roaming Between APs in Different Service VLANs

Like wired LANs, to prevent broadcast storms, enterprise users on enterprise WLANs are assigned different VLANs according to their floors and departments. If APs deployed at different floors belong to different VLANs, services of a user are interrupted when the user roams between two APs at different floors. Inter-VLAN Layer 3 roaming prevents service interruption in this case, improving WLAN service experience.

In roaming between APs in different service VLANs, APs before and after STA roaming belong to different service VLANs. To prevent services of a user from being interrupted during WLAN roaming, ensure that the service VLAN of the user remains unchanged after the user roams between two APs.

Figure 5-3 Roaming between APs in different service VLANs



You can classify roaming between APs in different service VLANs into fast roaming and non-fast roaming according to whether STAs support fast roaming. For the implementation principles of fast roaming and non-fast roaming, see **5.2.1 Roaming Between APs in the Same Service VLAN**. **Figure 5-3** describes how to keep the service VLAN of a STA unchanged during roaming of the STA.

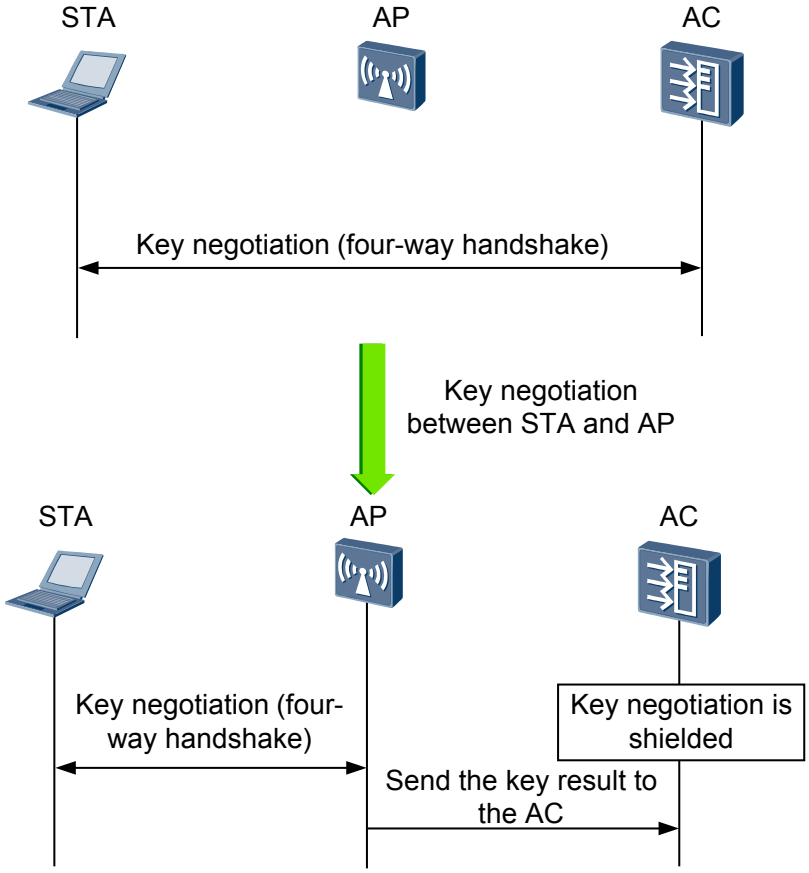
Figure 5-3 shows the process of roaming between APs in different service VLANs:

1. When the STA accesses the Internet through AP1 in VLAN 10, the AC determines that the STA accesses the Internet for the first time and creates and saves service data of the STA, including the service VLAN of the AP, AP ID, radio, and VAP information.
2. The STA moves from AP1 to AP2 in VLAN 20 and re-associates with the AC through AP2. The AC determines that the STA is roaming based on the user information, updates the service database, and updates the AP ID, radio, and VAP information to be consistent with AP2 information without changing the VLAN ID. The VLAN is still the service VLAN to which AP1 belongs.
3. The STA disassociates from AP1. Although the STA resides on different subnets after roaming between two APs, the AC still considers that the STA accesses the Internet from the first VLAN (VLAN 10), allowing the STA to retain its IP address to ensure nonstop service interruption.

5.2.3 Key Negotiation Between STA and AP

If a STA uses the WPA/WPA2 security policy, during roaming, the STA needs to perform key negotiation with an AC again. If the STA performs key negotiation with an AP, the roaming switchover time is reduced, implementing rapid roaming, as shown in **Figure 5-4**.

Figure 5-4 Key negotiation between STA and AP



In key negotiation between a STA and an AP, the STA sends a Re-association Request packet to the AP:

- If fast roaming is used, the AP sends the PMK-ID of the STA to the AC. The AC finds the PMK of the STA based on the PMK-ID and sends the PMK information to the AP. Subsequently, key negotiation is performed between the STA and AP. After the negotiation succeeds, the AP sends the key result to the AC.
- If non-fast roaming is used, the AC sends the generated PMK to the AP after the STA is re-authenticated through the AP. Subsequently, key negotiation is performed between the STA and AP. After the negotiation succeeds, the AP sends the key result to the AC.

5.3 References

The following table lists the references.

Document	Description	Remarks
IEEE 802.11r	WLAN roaming standard	-

6 WLAN QoS

About This Chapter

6.1 Introduction to WLAN QoS
6.2 Principles
6.3 Applications
6.4 References

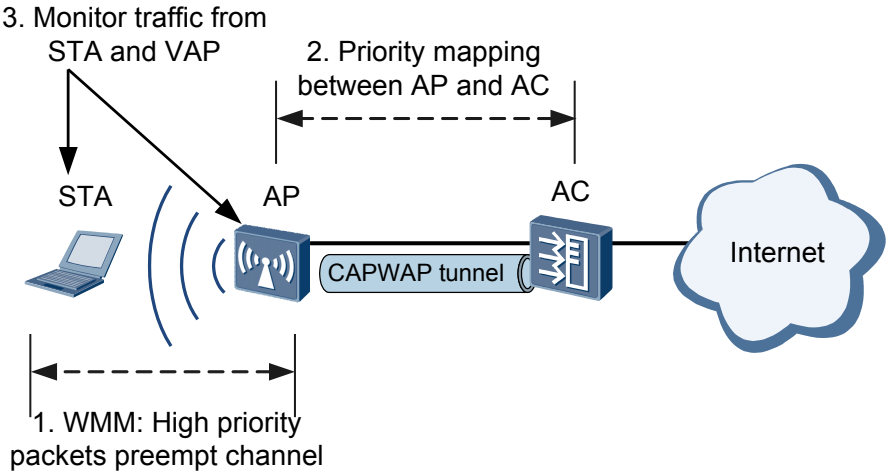
6.1 Introduction to WLAN QoS

Definition

WLAN Quality of Service (QoS) provides differentiated service for wireless users to satisfy their traffic requirements. As shown in **Figure 6-1**, WLAN QoS has the following functions:

1. High-efficiency use of wireless channels: The Wi-Fi multimedia (WMM) standard enables the high-priority users to preempt wireless channels.
2. Efficient bandwidth use: Priority mapping preferentially transmits the data of high-priority users.
3. Network congestion prevention: Traffic policing limits users' transmission rate, preventing network congestion.

Figure 6-1 WLAN QoS networking



Purpose

Applications have differentiated network requirements. The traditional WLAN is mainly used to transmit data due to its low transmission rate. With development of new WLAN technologies, WLANs have been applied to media, financial, education, and enterprise networks. In addition to data traffic, WLANs can also transmit delay-sensitive multimedia data, such as voice and video. By enforcing QoS policies on a WLAN, the network administrator can properly plan and assign network resources based on service characteristics. The WLAN then provides differentiated access services for applications, meeting customer requirements and improving network use efficiency.

6.2 Principles

6.2.1 WMM

Background

Before learning WMM, you must understand 802.11 link layer transport mechanism.

802.11 MAC layer uses the coordination function to determine the data transmitting and receiving methods used between STAs in a BSS. 802.11 MAC layer consists of two sub-layers:

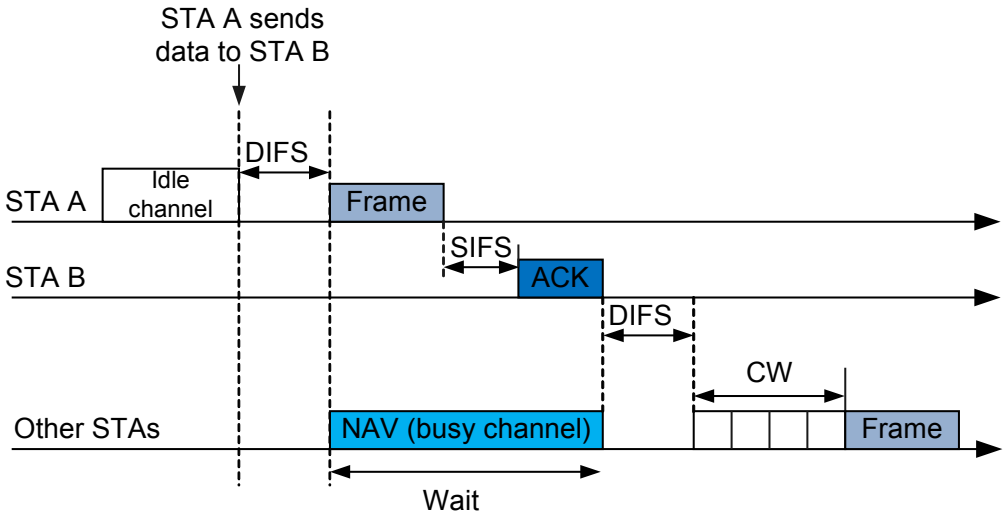
- Distributed Coordination Function (DCF): uses the CSMA/CA mechanism. STAs compete channels to obtain the authority to transmit data frames.
- Point Coordination Function (PCF): uses centralized control to authorize STAs to transmit data frames in turn. This method prevents conflict.

NOTE

In 802.11 protocol, DCF is mandatory, and PCF is optional.

Figure 6-2 shows how CSMA/CA is implemented.

Figure 6-2 CSMA/CA working mechanism



1. Before sending data to STA B, STA A detects channel status. When detecting an idle channel, STA A sends a data frame after Distributed Inter-Frame Space (DIFS) times out and waits for a response from STA B. The data frame contains NAV information. After receiving the data frame, STA B updates the NAV information, indicating that the channel is busy and data transmission will be delayed.

   NOTE

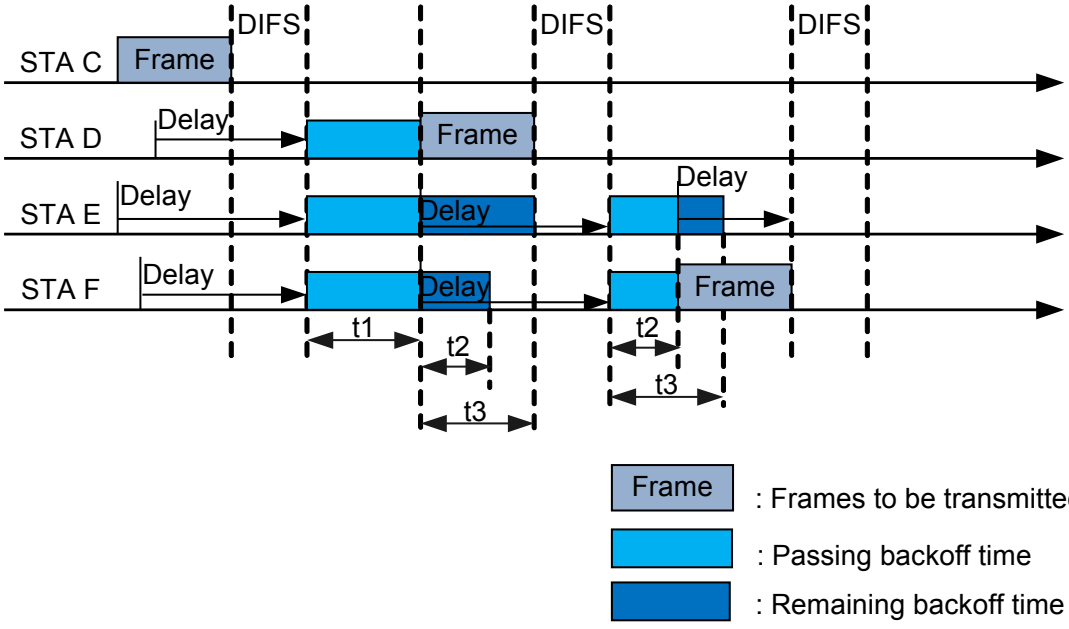
   According to 802.11 protocol, the receiver must return an ACK frame each time it receives a data frame.

2. STA B receives the data frame, waits until Short Interframe Space (SIFS) times out, and sends an ACK frame to STA A. After the ACK frame is transmitted, the channel becomes idle. After the DIFS times out, the STAs use the exponential backoff algorithm to compete channels. The STA of which the backoff counter is first reduced to 0 starts to send data frame.

Concepts

- InterFrame Space (IFS): According to 802.11 protocol, after sending a data frame, the STA must wait until the IFS times out, and then sends the next data frame. The IFS length depends on the data frame type. The high-priority data frames are sent earlier than the low-priority data frames. There are three IFS types:
  - Short IFS (SIFS): It is the time interval between a data frame and its ACK frame. SIFS is used for high priority transmissions, for example, transmissions of ACK and CTS frames.
  - PCF IFS (PIFS): PCF-enabled access points wait for PIFS duration rather than DIFS to occupy the wireless medium. PIFS length is SIFS plus slot time. If an STA accesses a channel when the slot time starts, the other STAs in the BSS detect that the channel is busy when the next slot time starts.
  - DCF IFS (DIFS): Data frames and management frames are transmitted at the DIFS interval. DIFS length is PIFS plus slot time.
- Contention window: backoff time. When multiple STAs need to transmit data and detect that all channels are busy, the STAs use the backoff algorithm. That is, the STAs wait for a random number of slot times, and then transmit data. Backoff time is a multiple of slot time, and its length depends on the physical layer technology. An STA detect channel status at the interval of slot time. When detecting an idle channel, the STA starts the backoff timer. If all channels become busy, the STA freezes the remaining time in the backoff timer. When a channel becomes idle, the STA waits until DIFS times out, and continues the backoff timer. When the backoff timer is reduced to 0, the STA starts to send data frames. **Figure 6-3** shows the data frame transmission process.

Figure 6-3 Backoff algorithm diagram



1. STA C is occupying a channel to send data frames. STA D, STA E, and STA F also need to send data frames. They detect that the channel is busy, so they wait.
2. After STA C finishes data frame transmission, the other STAs wait until DIFS times out. When DIFS times out, the STAs generate random backoff time and start their

backoff timers. For example, the backoff time of STA D is t1, the backoff time of STA E is t1+t3, and the backoff time of STA F is t1+t2.

3. When t1 times out, the backoff timer of STA D is reduced to 0. STA D starts to send data frames.
4. STA E and STA F detect that the channel is busy, so they freeze their backoff timers and wait. After STA D completes data transmission, STA E and STA F wait until DIFS times out, and continue their backoff timers.
5. When t2 times out, the backoff timer of STA F is reduced to 0. STA F starts to send data frames.

Principles

Channel competition is based on DCF. To all STAs, the DIFS is fixed and backoff time is random; therefore, all the STAs fairly compete channels. WMM is an enhancement to 802.11 protocol. It makes channel competition unfair.

- **EDCA parameters**

  WMM defines a set of Enhanced Distributed Channel Access (EDCA) parameters, which distinguish high priority packets and enables the high priority packets to preempt channels.

  WMM classifies data packets into four access categories (ACs). **Table 6-1** shows the mappings between ACs and 802.11 user preferences (UPs). A large UP value indicates a high priority.

  Table 6-1 Mappings between ACs and UPs

UP	AC
7	AC_VO (Voice)
6	
5	AC_VI (Video)
4	
3	AC_BE (Best Effort)
0	
2	AC_BK (Background)
1	

  Each AC queue defines a set of EDCA parameters, which determine the capability of occupying channels. These parameters ensure that the high priority ACs have higher probability to preempt channels than low priority ACs.

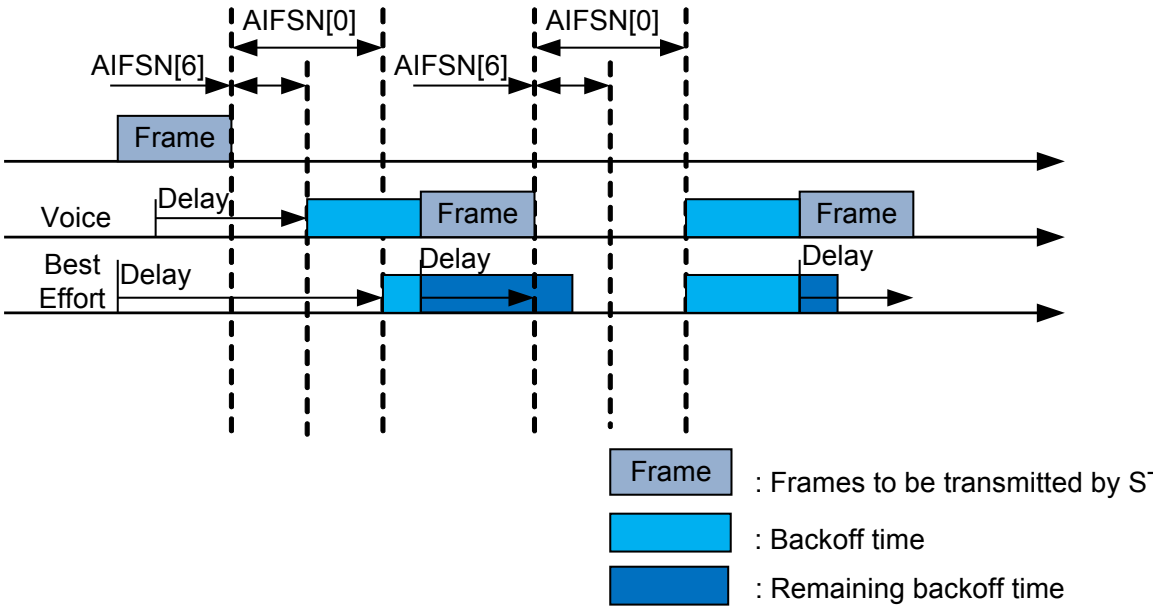
  Table 6-2 describes the EDCA parameters.

Table 6-2 EDCA parameter description

Parameter	Meaning
Arbitration Inter Frame Spacing Number (AIFSN)	The DIFS has a fixed value. WMM provides different DIFS values for different ACs. A large AIFSN value means that the STA must wait for a long time and has a low priority.
Exponent form of CWmin (ECWmin) and Exponent form of CWmax (ECWmax)	ECWmin specifies the minimum backoff time, and ECWmax specifies the maximum backoff time. They determine the average backoff time. Large ECWmin and ECWmax values mean that the average backoff time for the STA is long and the STA priority is low.
Transmission Opportunity Limit (TXOPLimit)	After preempting a channel, the STA can occupy the channel within the period of TXOPLimit. A large TXOPLimit value means that the STA can occupy the channel for a long time. If the TXOPLimit value is 0, the STA can send only one data frame every time it preempts a channel.

As shown in **Figure 6-4**, the AIFSN (AIFSN[6]) and backoff time of voice packets are shorter than those of Best Effort packets. When both voice packets and Best Effort packets need to be sent, voice packets can preempt the channel.

Figure 6-4 WMM working mechanism



- **ACK policy**

  WMM defines two ACK policies: normal ACK and no ACK.

- Normal ACK: The receiver must return an ACK frame each time it receives a unicast packet.
- No ACK: The receiver does not need to return ACK frames after receiving packets. This mode is applicable to the environment that has high communication quality and little interference.

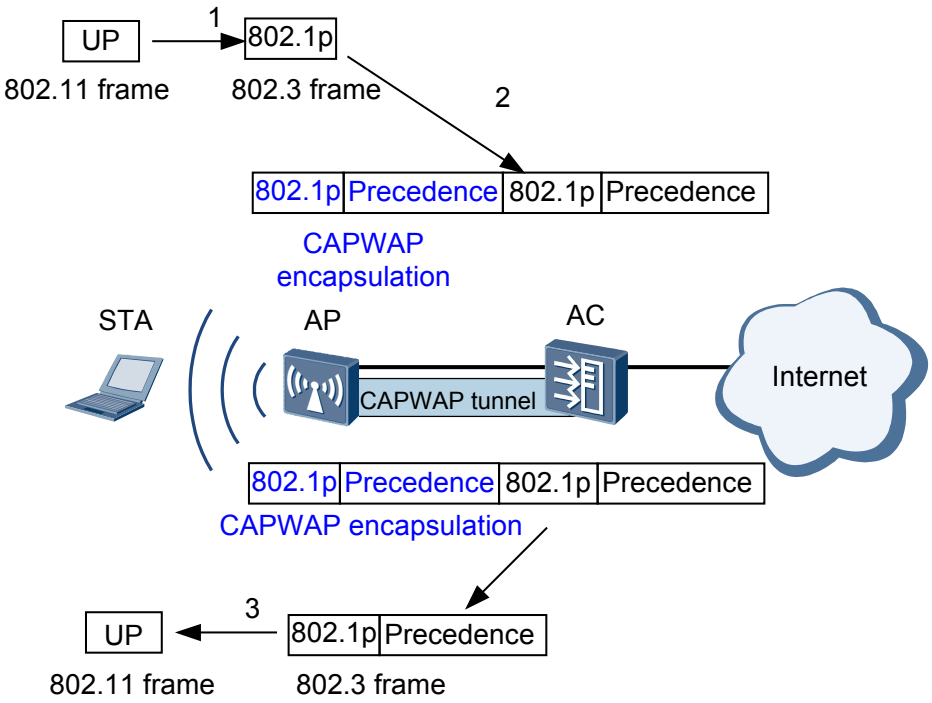
  NOTE

  - The ACK policy is only valid to APs.
  - If communication quality is poor, the no ACK policy may cause more packets to be lose.

6.2.2 Priority Mapping

Packets of different types have different priorities. For example, the 802.11 packets sent by STAs carry user preferences, VLAN packets on the wired networks carry 802.1p priorities, and IP packets carry precedence values or DSCP priorities. Priority mapping must be configured on network devices to retain priorities of packets when the packets traverse different networks.

Figure 6-5 Priority mapping diagram



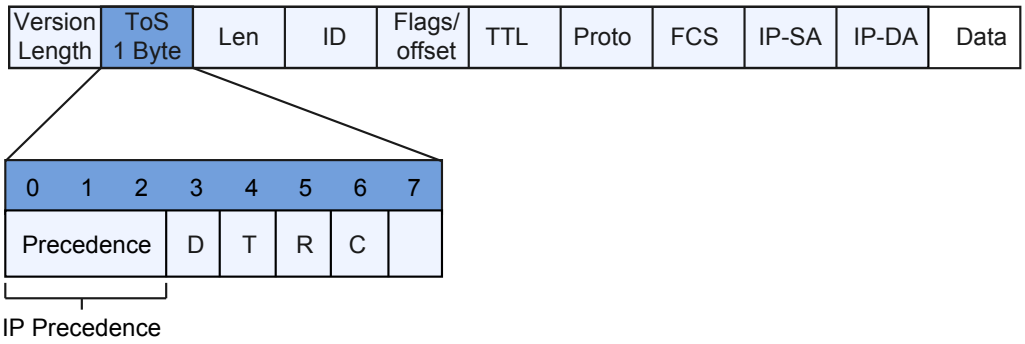
As shown in **Figure 6-5**:

1. After receiving the upstream 802.11 frames from the STA, the AP maps the user preferences to the 802.1p priorities.
2. In the upstream direction, if tunnel forwarding mode is used, the 802.1p priorities or precedence values must be mapped to tunnel priorities.
3. The AC forwards the 802.3 frames received from the Internet to the AP directly or through a tunnel. After receiving the downstream 802.3 frames, the AP maps the 802.1p priorities or precedence values to the user preference.

Precedence field

As defined in RFC 791, the 8-bit ToS field in an IP packet header contains a 3-bit IP precedence field. **Figure 6-6** shows the Precedence field in an IP packet. Bits 0 to 2 constitute the Precedence field, representing precedence values 7, 6, 5, 4, 3, 2, 1 and 0 in descending order of priority.

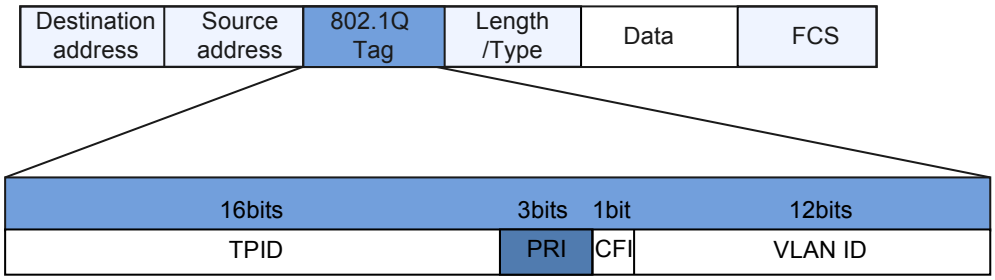
Figure 6-6 IP Precedence field



802.1p Field

Layer 2 devices exchange ethernet frames. As defined in IEEE 802.1Q, the PRI field (802.1p field) in the ethernet frame header identifies the Class of Service (CoS) requirement. **Figure 6-7** shows the PRI field in ethernet frames.

Figure 6-7 802.1p field in the Ethernet frame



The 802.1Q header contains a 3-bit PRI field, representing eight service priorities 7, 6, 5, 4, 3, 2, 1 and 0 in descending order of priority.

6.2.3 Traffic Policing

Traffic policing discards excess traffic to limit the traffic within a specified range and to protect network resources as well as the enterprise benefits.

Traffic policing is implemented using the token bucket.

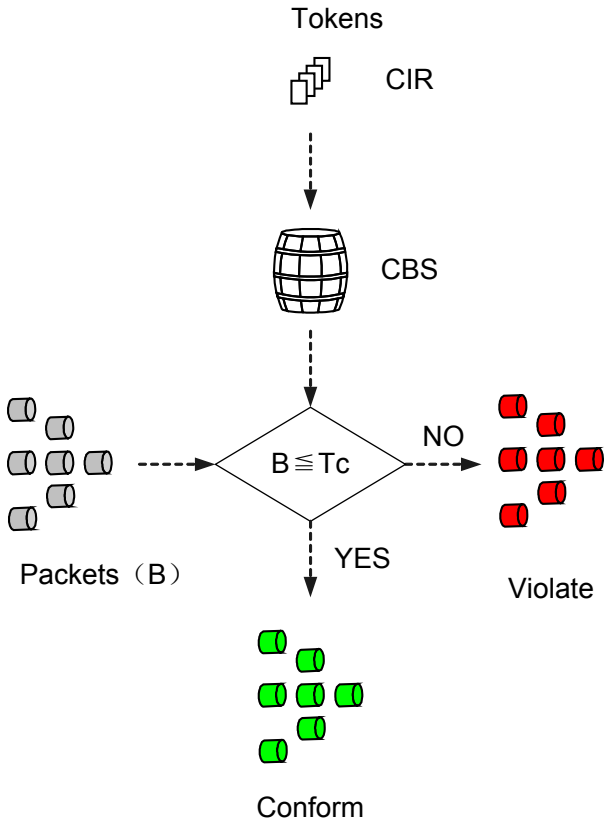
A token bucket has specified capacity to store tokens. The system places tokens into a token bucket at the configured rate. If the token bucket is full, excess tokens overflow and no token is added.

When assessing traffic, a token bucket forwards packets based on the number of tokens in the token bucket. If there are enough tokens in the token bucket for forwarding packets, the traffic rate is within the rate limit. Otherwise, the traffic rate is not within the rate limit.

The working mechanisms of token buckets include single rate single bucket, single rate dual bucket, and dual rate dual bucket.

Single Bucket at a Single Rate

Figure 6-8 Single bucket at a single rate



As shown in **Figure 6-8**, the bucket is called bucket C. Tc indicates the number of tokens in bucket C. A single bucket at a single rate uses the following parameters:

- Committed information rate (CIR): indicates the rate at which tokens are put into bucket C, that is, average traffic rate permitted by bucket C.
- Committed burst size (CBS): indicates the capacity of bucket C, that is, maximum volume of burst traffic allowed by bucket C each time.

The system places tokens into the bucket at the CIR. If Tc is smaller than the CBS, Tc increases. If Tc is larger than or equal to the CBS, Tc remains unchanged.

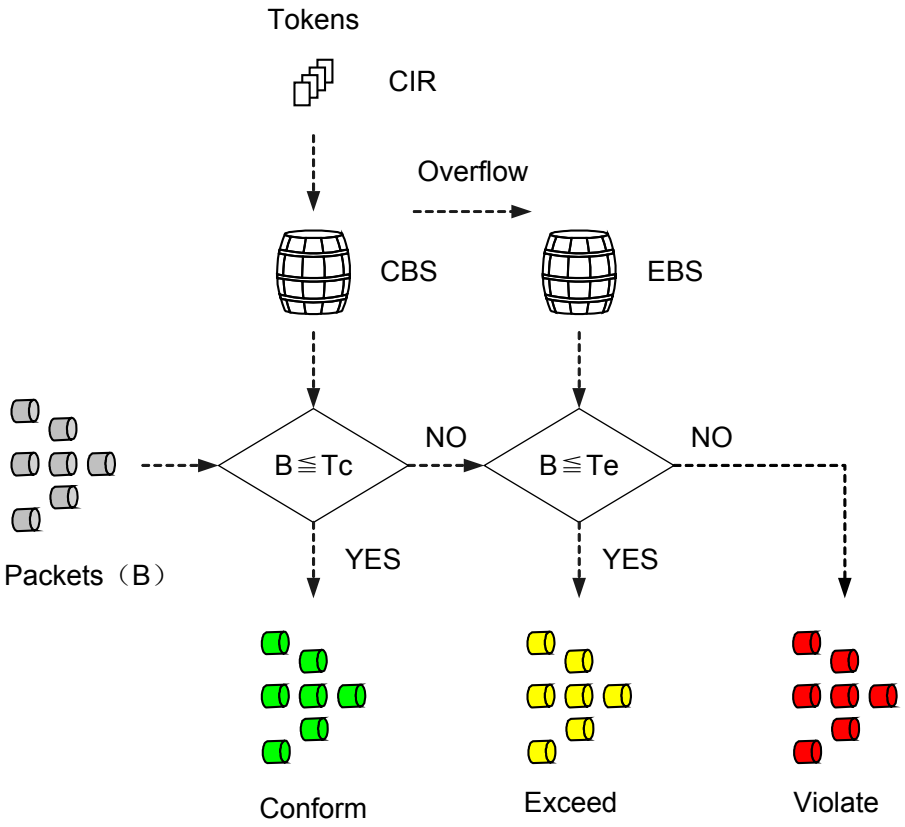
B indicates the size of an arriving packet:

- If B is smaller than or equal to Tc, the packet is colored green, and Tc decreases by B.
- If B is larger than Tc, the packet is colored red, and Tc remains unchanged.

Dual Buckets at a Single Rate

Dual buckets at a single rate use A Single Rate Three Color Marker (srTCM) defined in RFC 2697 to assess traffic and mark packets in green, yellow, and red based on the assessment result.

Figure 6-9 Dual buckets at a single rate



As shown in **Figure 6-9**, the two buckets are called bucket C and bucket E. Tc indicates the number of tokens in bucket C, and Te indicates the number of tokens in bucket E. Dual buckets at a single rate use the following parameters:

- CIR: indicates the rate at which tokens are put into bucket C, that is, average traffic rate permitted by bucket C.
- CBS: indicates the capacity of bucket C, that is, maximum volume of burst traffic allowed by bucket C each time.
- Excess burst size (EBS): indicates the capacity of bucket E, that is, maximum volume of excess burst traffic allowed by bucket E each time.

The system places tokens into the bucket at the CIR:

- If Tc is smaller than the CBS, Tc increases.
- If Tc is equal to the CBS and Te is smaller than the EBS, Te increases.
- If Tc is equal to the CBS and Te is equal to the EBS, Tc and Te do not increase.

B indicates the size of an arriving packet:

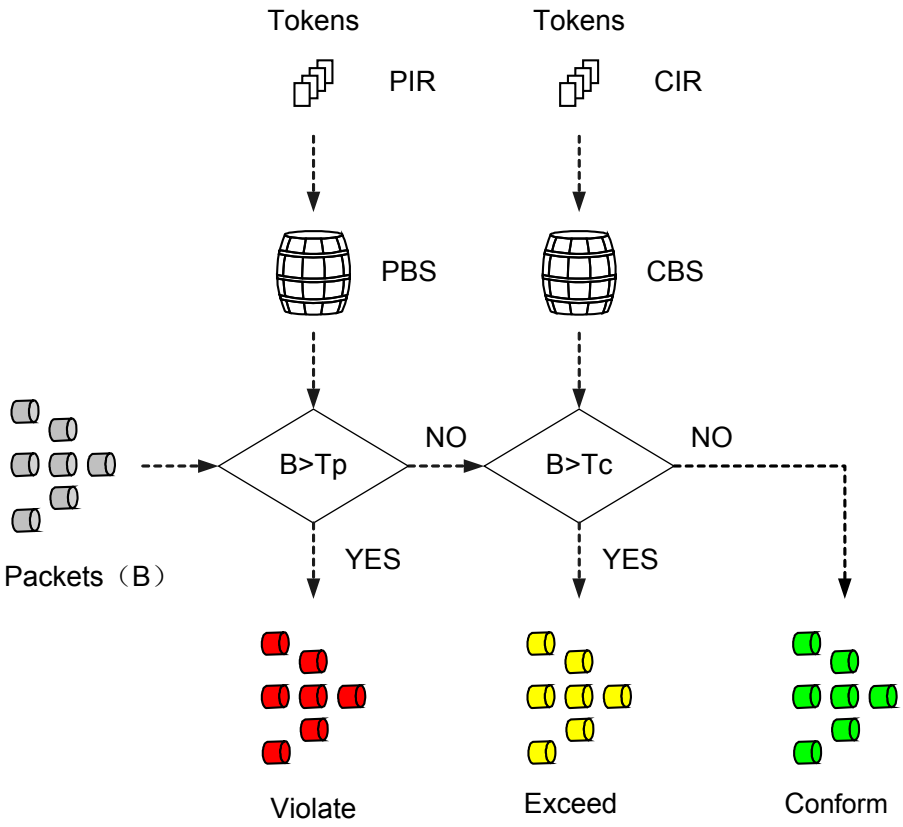
- If B is smaller than or equal to Tc, the packet is colored green, and Tc decreases by B.

- If B is larger than Tc and smaller than or equal to Te, the packet is colored yellow and Te decreases by B.
- If B is larger than Te, the packet is colored red, and Tc and Te remain unchanged.

Dual Buckets at Dual Rates

Dual buckets at dual rates use A Two Rate Three Color Marker (trTCM) defined in RFC 2698 to assess traffic and mark packets in green, yellow, and red based on the assessment result.

Figure 6-10 Dual buckets at dual rates



As shown in **Figure 6-10**, the two buckets are called bucket P and bucket C. Tp indicates the number of tokens in bucket P, and Tc indicates the number of tokens in bucket C. Dual buckets at dual rates use the following parameters:

- Peak information rate (PIR): indicates the rate at which tokens are put into bucket P, that is, average traffic rate permitted by bucket P. The PIR must be greater than the CIR.
- CIR: indicates the rate at which tokens are put into bucket C, that is, average traffic rate permitted by bucket C.
- Peak burst size (PBS): indicates the capacity of bucket P, that is, maximum volume of burst traffic allowed by bucket P each time.
- CBS: indicates the capacity of bucket C, that is, maximum volume of burst traffic allowed by bucket C each time.

The system places tokens into bucket P at the PIR and places tokens into bucket C at the CIR:

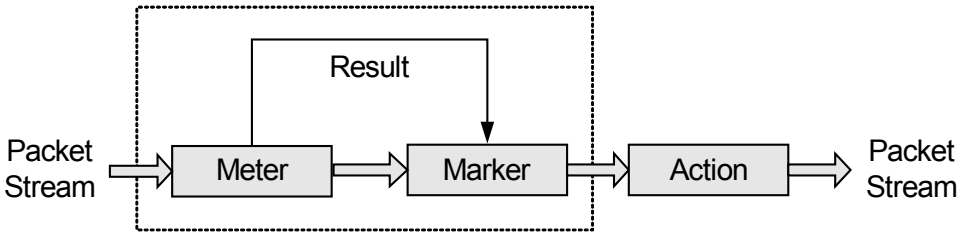
- If Tp is smaller than the PBS, Tp increases. If Tp is larger than or equal to the PBS, Tp remains unchanged.
- If Tc is smaller than the CBS, Tc increases. If Tc is larger than or equal to the CBS, Tp remains unchanged.

B indicates the size of an arriving packet:

- If B is larger than Tp, the packet is colored red.
- If B is larger than Tc and smaller than or equal to Tp, the packet is colored yellow and Tp decreases by B.
- If B is smaller than or equal to Tc, the packet is colored green, and Tp and Tc decrease by B.

Implementation of Traffic Policing

Figure 6-11 Traffic policing components



As shown in **Figure 6-11**, traffic policing involves the following components:

- Meter: measures the network traffic using the token bucket mechanism and sends the measurement result to the marker.
- Marker: colors packets in green, yellow, or red based on the measurement result received from the meter.
- Action: performs actions based on packet coloring results received from the marker. The following actions are defined:
  - Pass: forwards the packets that meet network requirements.
  - Remark + pass: changes the local priorities of packets and forwards them.
  - Discard: drops the packets that do not meet network requirements.

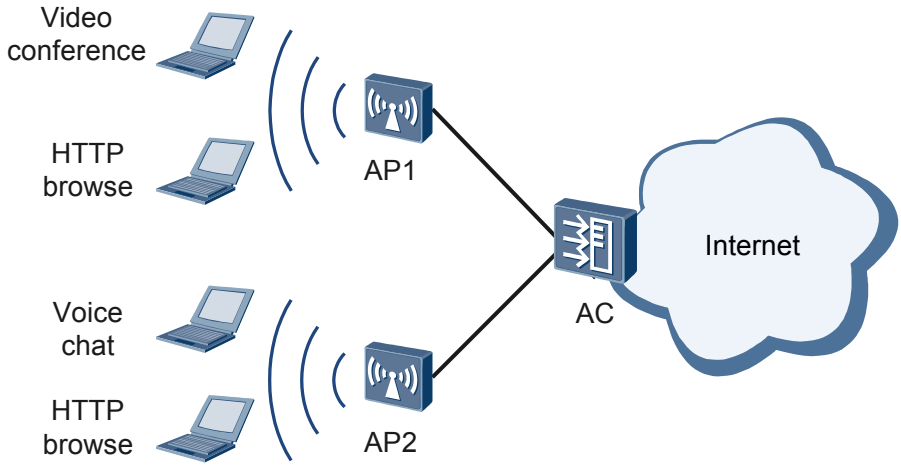
  By default, green and yellow packets are forwarded, and red packets are discarded.

If the rate of a type of traffic exceeds the threshold, the device reduces the packet priority and then forwards the packets or directly discards the packets based on traffic policing configuration. By default, the packets are discarded.

6.3 Applications

As shown in **Figure 6-12**, network bandwidth is limited. The device needs to provide differentiated services for services, for example, reducing jitter and latency of voice packets and guaranteeing bandwidth for key services.

Figure 6-12 WLAN QoS networking diagram



- By using WMM, voice or video data can preempt wireless channels.
- By using priority mapping, high priority data is transmitted first.
- By using traffic policing, user data rate is limited and network congestion is prevented.

6.4 References

The following table lists the references.

Document	Description	Remarks
IEEE 802.11e	Support on QoS	-

7 WLAN WDS

About This Chapter

7.1 Introduction to WDS

7.2 Principles

7.3 Applications

7.4 References

7.1 Introduction to WDS

Definition

A wireless distribution system (WDS) connects two or more wired or wireless LANs wirelessly to establish a large network.

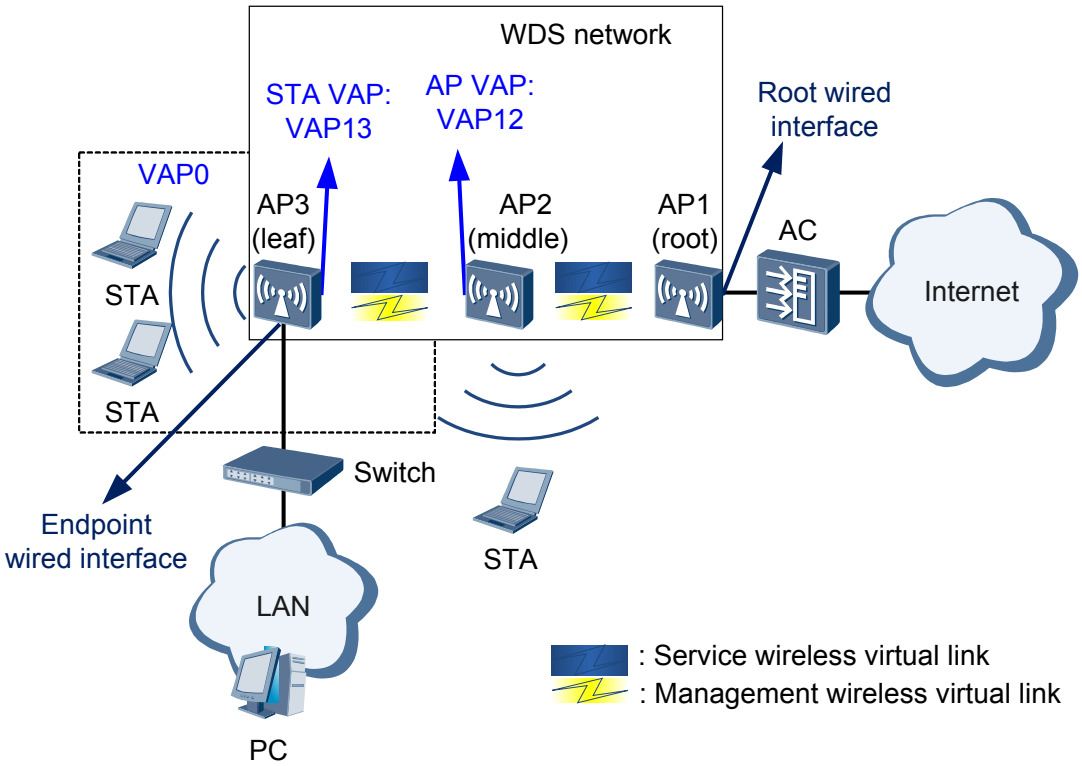
Purpose

On a traditional WLAN, APs exchange data with STAs using wireless channels and connect to a wired network through uplinks. To expand the coverage area of a wireless network, APs need to be connected by switches. This deployment requires high costs and takes a long time. In some places, such as subways, tunnels, and docks, it is difficult to connect APs to the Internet through wired links. WDS technology can connect APs wirelessly in these places, which reduces network deployment costs, makes the network easy to expand, and allows flexible networking.

7.2 Principles

WDS Concepts

Figure 7-1 WDS networking



- Service VAP: On a traditional WLAN, an AP is a physical entity that provides WLAN services to STAs. A service virtual access point (VAP) is a logical entity that provides access service for users. Multiple VAPs can be created on an AP to provide access service for multiple user groups. As shown in **Figure 7-1**, VAP0 created on AP3 is a service VAP.

  NOTE

  When you create service VAPs, the system allocates VAPs to service sets in sequence, starting from VAP0 by default. That is, the system allocates VAP0 to the first service set and VAP1 to the second service set.

- Bridge VAP: On a WDS network, an AP is a physical entity that provides WDS service for neighboring devices. A bridge VAP is a logical entity that provides WDS service. Bridge VAPs include AP VAPs and STA VAPs, which work in pairs. AP VAPs provide connections for STA VAPs. As shown in **Figure 7-1**, VAP13 created on AP3 is a STA VAP, and VAP12 created on AP2 is an AP VAP.
- Wireless virtual link: a connection set up between a STA VAP and an AP VAP on neighboring APs. As shown in **Figure 7-1**, connections set up between AP1, AP2, and AP3 are wireless virtual links. Wireless virtual links include service wireless virtual links and management wireless virtual links.
  - Service wireless virtual link: a wireless virtual link that forwards user data on a WDS network.
  - Management wireless virtual link: a wireless virtual link that forwards management and control packets on a WDS network. A management wireless virtual link is used to control link setup and deliver configuration parameters.
- AP working mode: Depending on its location on a WDS network, an AP can work in root, middle, or leaf mode, as shown in **Figure 7-1**.
  - Root: The AP directly connects to an AC through a wired link and uses an AP VAP to set up wireless virtual links with a STA VAP.
  - Middle: The AP uses a STA VAP to connect to an AP VAP on an upstream AP and uses an AP VAP to connect to a STA VAP on a downstream AP.
  - Leaf: The AP uses a STA VAP to connect to an AP VAP on an upstream AP.
- Working mode of an AP's wired interface: On a WDS network, an AP's wired interface can connect to either an upstream wired network or a downstream user host or LAN. Depending on an AP's location, a wired interface works in root or endpoint mode.
  - Root: The wired interface connects to an upstream wired network.
  - endpoint: The wired interface connects to a downstream user host or LAN.

  NOTE

  On a WDS network, one wired interface must work in root mode to connect to the wired network.

WDS Implementation

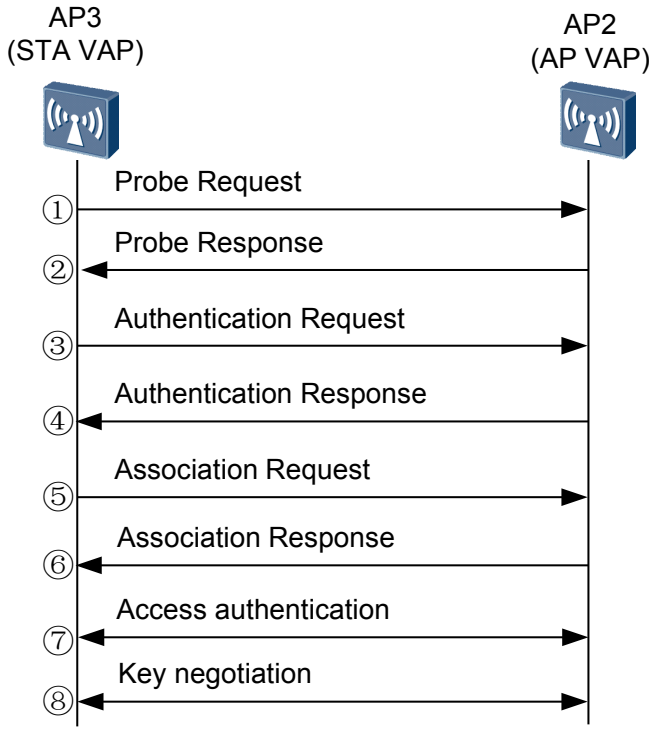
- Setting up a management wireless virtual link

  After WDS is enabled on an AP, the AP automatically creates two bridge VAPs, one AP VAP and one STA VAP. The AP uses the bridge VAPs to set up wireless virtual links with other APs. After management wireless virtual links are set up, APs connect to the AC through the management wireless virtual links and obtain configurations from the AC.

- Setting up a service wireless virtual link

  Figure 7-2 shows how a service wireless virtual link is set up between AP2 and AP3 on the WDS network shown in **Figure 7-1**.

Figure 7-2 Setting up a service wireless virtual link



1. Probe request

   AP3 broadcasts a Probe Request frame carrying a Bridge-Name field (similar to SSID in WLAN service).

2. Probe response

   AP2 receives the Probe Request frame and sends a Probe Response frame to AP3.

3. Authentication request

   After AP3 receives the Probe Response frame, it sends an Authentication Request frame to AP2.

4. Authentication response

   After AP2 receives the Authentication Request frame, it determines whether to allow access from AP3 depending on the bridge whitelist configuration:

   - If bridge whitelist is not enabled, AP2 allows access from AP3 and sends an Authentication Response frame to notify AP3 that the authentication succeeds.
   - If bridge whitelist is enabled, AP2 checks whether the MAC address of AP3 is included in the bridge whitelist.
     - If the MAC address of AP3 is included in the bridge whitelist, AP2 allows access from AP3 and sends an Authentication Response frame to notify AP3 that the authentication succeeds.
     - If the MAC address of AP3 is not included in the bridge whitelist, AP2 sends an Authentication Response frame with an error code, indicating that the authentication fails. The process ends and the service wireless virtual link cannot be set up.

5. Association request

After AP3 receives the Authentication Response frame indicates an authentication success, it sends an Association Request frame to AP2.

6. Association response

   After AP2 receives the Association Request frame, it sends an Association Response frame to request AP3 to start the access authentication.

7. Access authentication

   On a WDS network, the access authentication method for a STA VAP must be WPA2-PSK. Therefore, AP3 and AP2 use a pre-configured shared key for negotiation. If they can decrypt messages sent from each other using the shared key, they have the same shared key and the access authentication succeeds.

8. Key negotiation

   AP3 and AP2 negotiate an encryption key to encrypt service packets.

NOTE

- After a service wireless virtual link is set up, APs periodically send link status messages to each other. If one AP does not receive any link status message from the other AP within a specified period, it terminates the service wireless virtual link and starts to set up a new service wireless virtual link.
- If the AC delivers new WDS parameter settings to APs, the APs use the new parameter settings to set up service wireless virtual links.

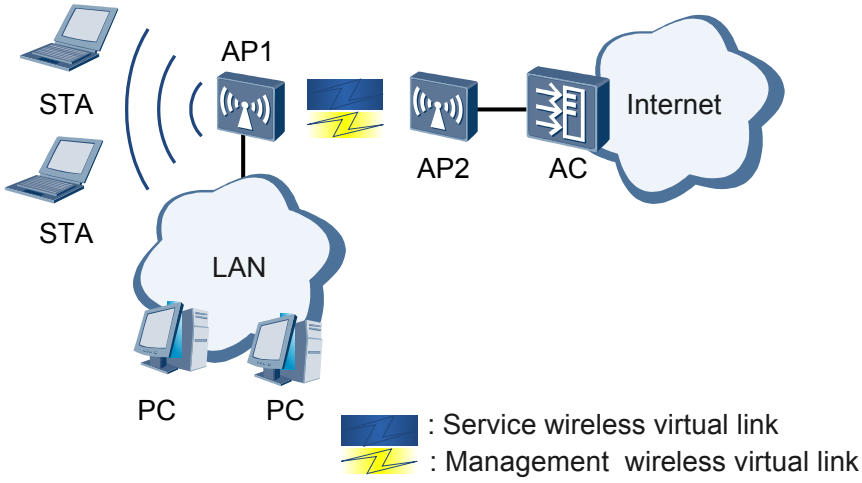
WDS Network Architecture

A WDS network can be deployed in point-to-point or point-to-multipoint mode.

- Point-to-point deployment

  As shown in **Figure 7-3**, AP1 sets up wireless virtual links with AP2 to provide wireless access service for users.

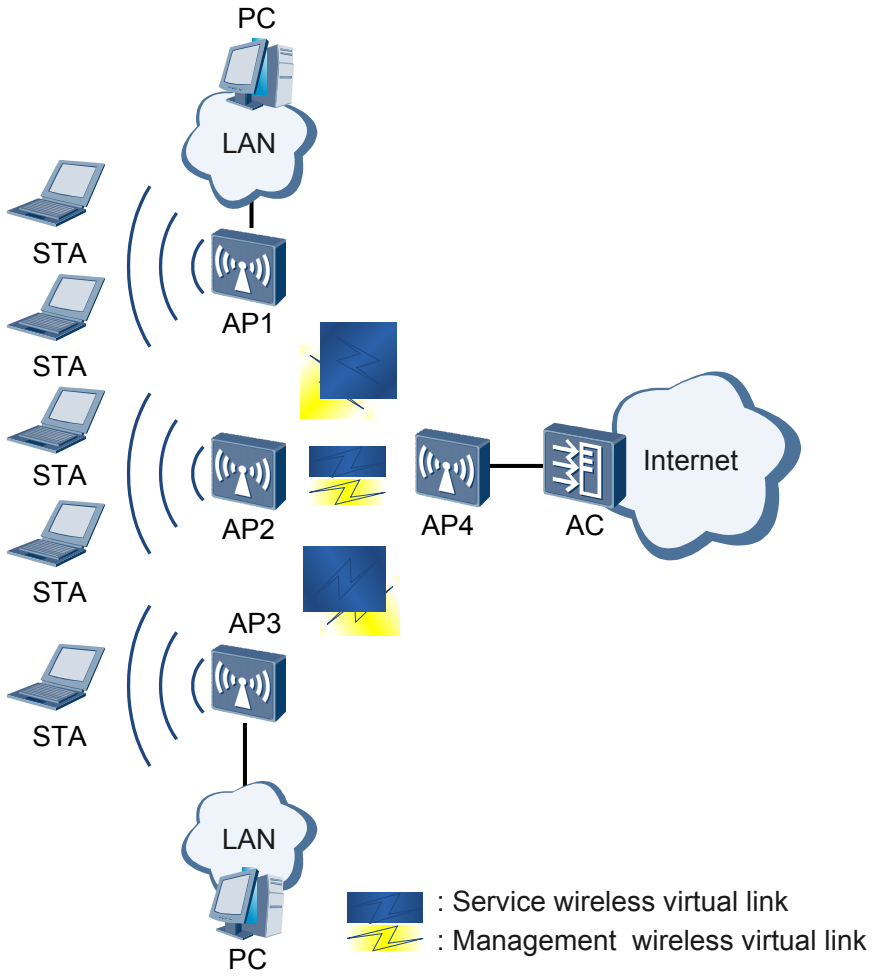
  Figure 7-3 Point-to-point WDS deployment



- Point-to-multipoint deployment

  As shown in **Figure 7-4**, AP1, AP2, and AP3 set up wireless virtual links with AP4. Data from all STAs associating with AP1, AP2, and AP3 is forwarded by AP4.

Figure 7-4 Point-to-multipoint WDS deployment



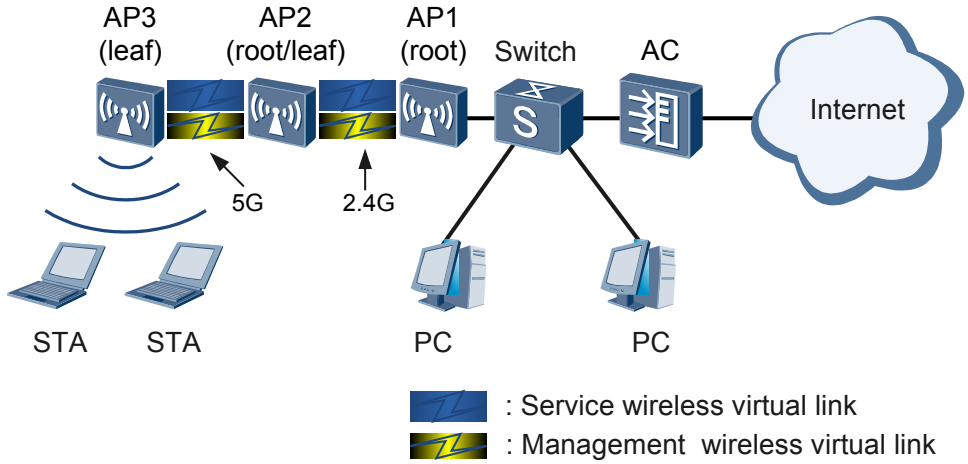
7.3 Applications

In WDS application, APs can be deployed in the hand-in-hand or back-to-back mode.

Hand-in-Hand WDS Networking

As shown in **Figure 7-5**, AP1 is a single-band AP that works at 2.4 GHz frequency band; AP2 and AP3 are all dual-band APs. AP1 and AP2 use 2.4 GHz radio to set up wireless virtual links (WVLs), while AP2 and AP3 use 5 GHz radio to set up WVLs. AP3 connects STAs to the WLAN through the 2.4 GHz radio. On a hand-in-hand WDS network, AP1, AP2, and AP3 use different radios to set up WVLs.

Figure 7-5 Hand-in-hand WDS networking applications



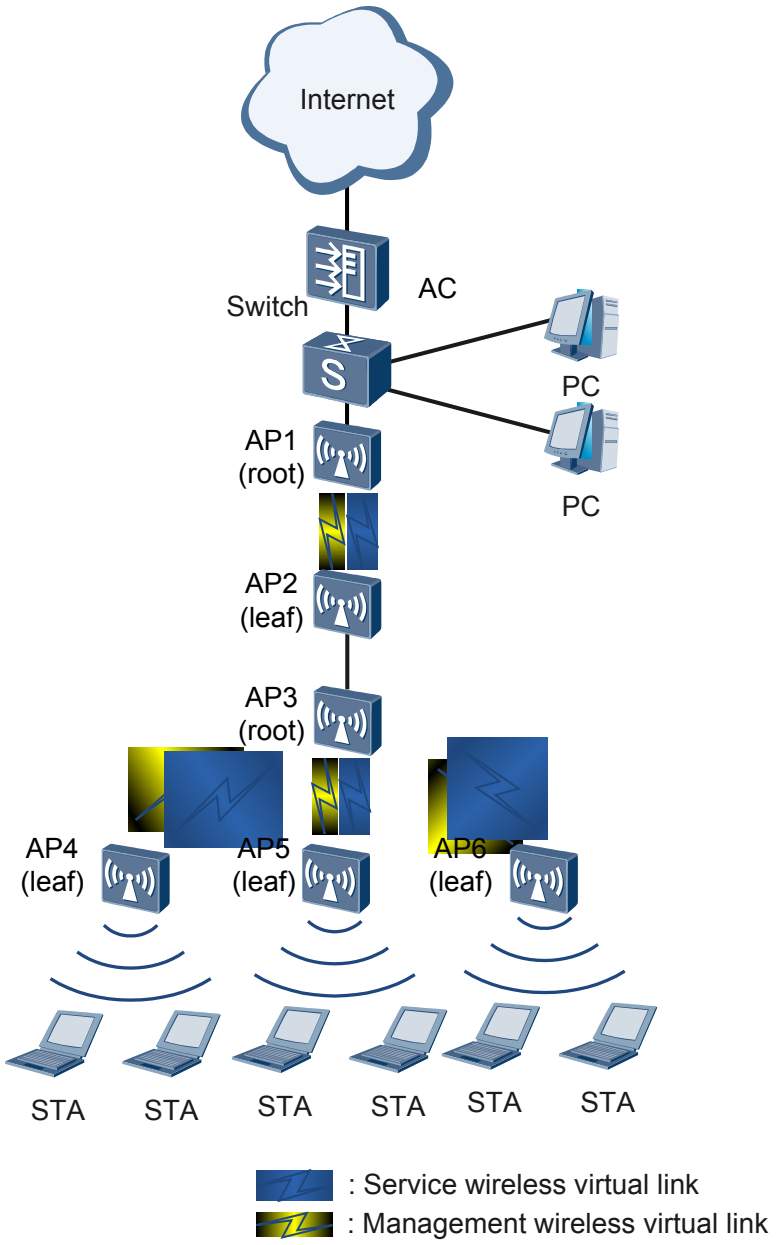
NOTE

In the figure, AP2 on 2.4 GHz radio functions as a leaf node for AP1 and AP2 on 5 GHz radio functions as a root node for AP3.

Back-to-Back WDS Networking

In outdoor scenarios, such as school campus, plantations, and mountain areas, wired networks are difficult to deploy. When networks to be connected are far from each other or blocked by obstacles, APs can be cascaded as trunk bridges in back-to-back mode. This networking ensures sufficient bandwidth on wireless links for long distance data transmission. **Figure 7-6** shows the back-to-back WDS networking.

Figure 7-6 Back-to-back WDS networking



7.4 References

The following table lists the reference for this feature.

Document	Description	Remarks
IEEE 802.11	Wireless LAN communications standards	-

8 WLAN Mesh

About This Chapter

8.1 Introduction to WLAN Mesh
8.2 Principles
8.3 Applications
8.4 References

8.1 Introduction to WLAN Mesh

Definition

A wireless mesh network (WMN) is a communications network that consists of multiple wirelessly connected APs in a mesh topology and connects to a wired network through a portal node or two portal nodes.

Purpose

On a traditional WLAN, APs exchange data with STAs using wireless channels and connect to a wired network through uplinks. If no wired network is available before a WLAN is constructed, it takes much time and money to construct a wired network. If positions of some APs on a WLAN are adjusted, the wired network must be adjusted accordingly, increasing the difficulty in network adjustment. A traditional WLAN requires a long construction period and has a high cost and poor flexibility, so it does not apply to emergency communication, wireless MANs, or areas that lack weak wired network infrastructure. The construction of a WMN requires only APs to be installed, which greatly speeds up network construction.

A WMN allows APs to wirelessly connect to each other, solving the preceding problems. A WMN has the following advantages:

- Fast deployment: Mesh nodes can be easily installed to construct a WMN in a short time, much shorter than the construction period of a traditional WLAN.
- Dynamic coverage area expansion: As more mesh nodes are deployed on a WMN, the WMN coverage area can be rapidly expanded.
- Robustness: A WMN is a peer network that will not be affected by the failure of a single node. If a node fails, packets are forwarded to the destination node along the backup path.
- Flexible networking: An AP can join or leave a WMN easily, allowing for flexible networking.
- Various application scenarios: Besides traditional WLAN scenarios such as enterprise networks, office networks, and campus networks, a WMN also applies to scenarios such as large-scale warehouses, docks, MANs, metro lines, and emergency communications.
- Cost-effectiveness: Only MPPs need to connect to a wired network, which minimizes the dependency of a WMN on wired devices and saves costs in wired device purchasing and cable deployment.

Benefits

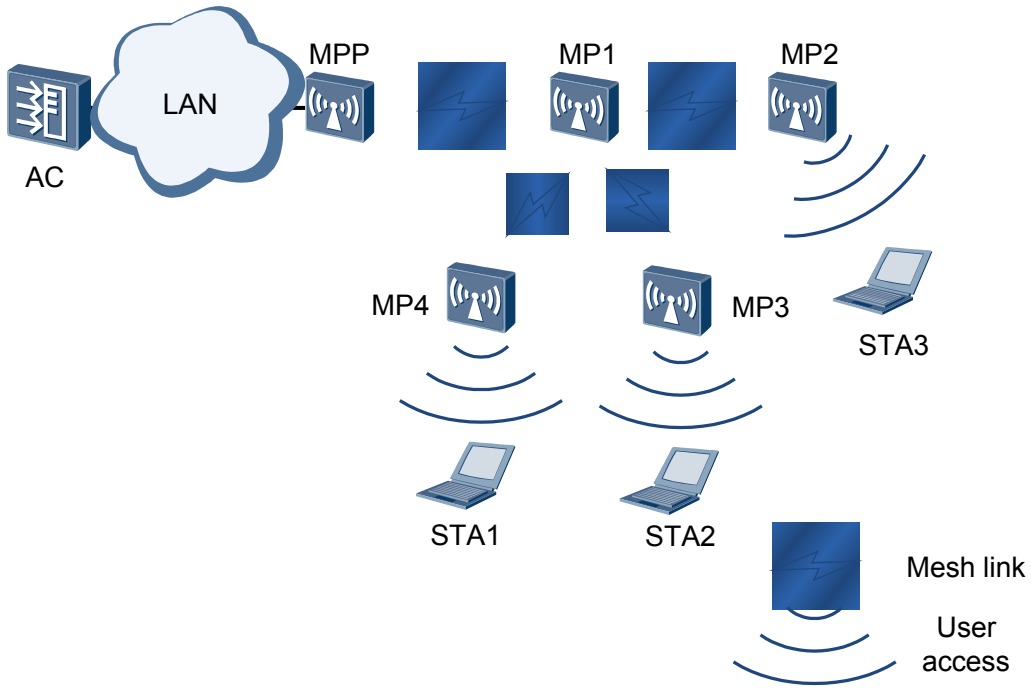
A WMN saves cables required between mesh nodes while providing path redundancy and rerouting functions as a distributed network. Therefore,

- When a new AP is added to a WMN, the AP can automatically connect to the WMN and determine the optimal multi-hop transmission path after being powered on.
- When an AP is moved from a WMN, the WMN can automatically discover the topology change and adjust communication routes to obtain the optimal transmission path.

8.2 Principles

Concepts

Figure 8-1 Networking diagram



A WMN includes the following devices:

- Mesh point (MP): a mesh-capable node that uses IEEE 802.11 MAC and physical layer protocols for wireless communication. This node supports automatic topology discovery, automatic route discovery, and data packet forwarding. MPs can provide both mesh service and user access service.
- Mesh point portal (MPP): an MP that connects to a WMN or another type of network. This node has the portal function and enables mesh nodes to communicate with external networks.
- Neighboring MP: an MP that directly communicates with another MP or MPP. For example, in **Figure 8-1**, MP2 is the neighbor of MP1.
- Candidate MP: a neighboring MP with which an MP prepares to establish a mesh link.
- Peer MP: a neighboring MP that has established a mesh connection with an MP.

Implementation

The establishment of a mesh link includes mesh neighbor discovery and mesh connection management.

MESH NEIGHBOR DISCOVERY

1. Discover a mesh neighbor.

   Before constructing a WMN, an MP needs to discover neighboring MPs. An MP can obtain neighboring MP information through active or passive scanning, similar to STA access to WLANs.

- Active scanning: An MP periodically sends a wildcard Mesh Probe Request frame (a mesh management frame with the SSID length 0) in a specified channel to search for a neighboring MP.
- Passive scanning: An MP listens on the Mesh Beacon frames sent from neighboring MPs in each channel to obtain neighboring MP information. A Beacon frame contains information including the Mesh ID.

2. Update the neighbor relationship table.

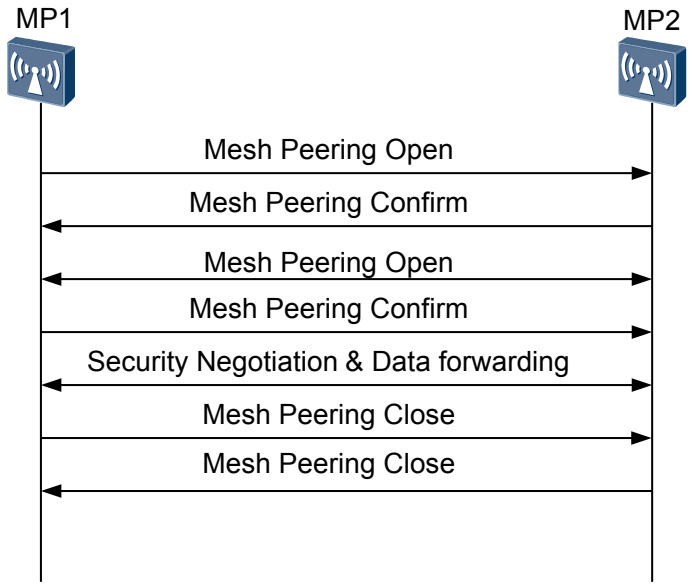
   Each MP has a neighbor relationship table that contains information about four types of neighboring nodes: common AP neighbors, nodes of other WMNs, candidate MPs, and peer MPs.

   - In active scanning, if a neighboring MP finds that the received Mesh Probe Request frame is a wildcard frame, it sends a Mesh Probe Response frame that contains the Mesh ID and other required information to the MP. The MP checks whether the Mesh ID in the received Mesh Probe Response frame is the same as the local Mesh ID. If the two Mesh IDs are the same, the MP records the neighboring MP as a candidate MP in the neighbor relationship table.
   - In passive scanning, if the MP finds that the Mesh ID in the Mesh Beacon frame received from a neighboring MP is the same as the local Mesh ID, the MP records the neighboring MP as a candidate MP in the neighbor relationship table.

Mesh Connection Management

Mesh connection management involves two phases: mesh connection establishment and mesh connection teardown. The two phases are implemented using three types of Mesh Action frames: Mesh Peering Open, Mesh Peering Confirm, and Mesh Peering Close frames.

Figure 8-2 Mesh connection management process



1. Mesh connection establishment

   An MP can initiate a mesh connection with a candidate MP. The two MPs are peers and exchange Mesh Peering Open and Mesh Peering Confirm frames to establish a mesh connection.

After the two MPs establish a mesh connection, they start the key negotiation phase. The two MPs can forward mesh data only after key negotiation succeeds.

2. Mesh connection teardown

   Either of the two MPs that establish a mesh connection can send a Mesh Peering Close frame to the other MP to tear down the mesh connection. After receiving the Mesh Peering Close frame, the other MP needs to respond with a Mesh Peering Close frame.

Mesh Routing

On a WMN, multiple mesh links are available between any source and destination, and the transmission quality of these mesh links varies according to the surrounding environment. Therefore, routing protocols are required on the WMN. The Hybrid Wireless Mesh Protocol (HWMP) defined in the 802.11s standard can address routing issues.

The following route management frames are defined in HWMP:

- Root Announcement (RANN) frame: used to announce the presence of an MPP.
  - An MPP periodically broadcasts a RANN frame.
  - After an MP receives a RANN frame, the MP reduces the time to live (TTL) of the frame by 1, updates the path metric, and broadcasts the frame. After an MP reads a RANN frame, the MP checks whether the gateway specified in the RANN frame exists in the local gateway list. If the gateway exists in the local gateway list, the MP updates the gateway information in the gateway list according to the information in the RANN frame. Otherwise, the MP adds gateway information to the gateway list.
- Proxy Update (PU) and Proxy Update Confirm (PUC) frames
  - An MP sends a PU frame to an MPP periodically or when the MP detects changes of its associated STA. The PU frame contains information about the STA associating with the MP.
  - The MPP sends a PUC frame to the MP after receiving the PU frame from the MP.
- Route Request (RREQ) and Route Reply (RREP) frames: In on-demand routing mode, the source node broadcasts a RREQ frame to establish a route to the destination node. After an MP receives the RREQ frame, the MP responds with a RREP frame.

A WMN supports two routing modes: on-demand routing and proactive routing.

- On-demand routing: The source node broadcasts a RREQ frame to establish a route to the destination node. After receiving the RREQ frame, a transit node checks the frame. If the RREQ frame contains a sequence number larger than or equal to the sequence number of the previous frame but has a lower metric, the transit node creates and updates the route to the source node. If the transit node has no route to the destination route, the transit node continues forwarding the RREQ frame.
- Proactive routing: A root node periodically broadcasts a RANN frame. When a mesh node receives a RANN frame and needs to create or update the route to the root node, the mesh node unicasts a RREP frame to the root node and broadcasts the RANN frame. Then, the root node creates a reverse path from the root node to the source node, and the mesh node creates a forwarding path from the root node to the source node.

HWMP combines on-demand routing and proactive routing to ensure that data frames are always transmitted on mesh links with the best transmission quality.

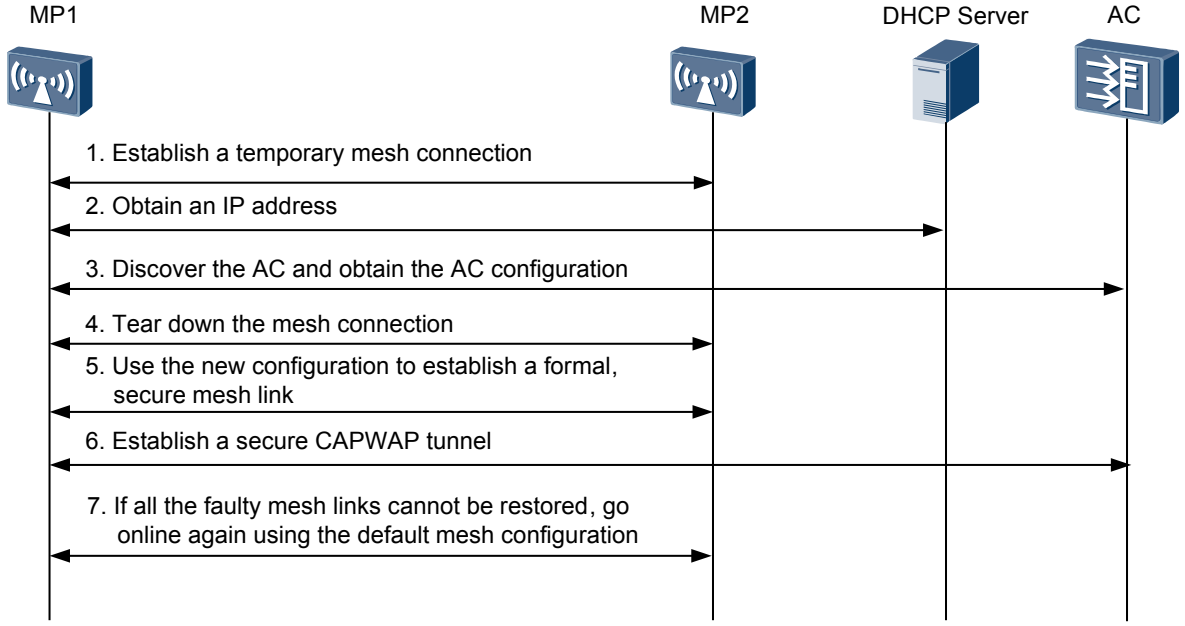
Huawei develops and optimizes the proprietary mesh routing protocol based on the 802.11s standard to implement route load balancing. The mesh routing protocol has the following characteristics:

- Reduces the number of times frames are forwarded during the wireless link establishment and constructs the forwarding topology based on the path with the minimum hops from the source node to the destination node.
- Selects paths dynamically based on the link-quality parameters including the expected transmission count (ETX) and expected transmission time (ETT) to implement load balancing.

Zero Touch Configuration

On a WMN that uses the centralized WLAN architecture (AC+Fit AP), you only need to perform a few AP management configurations on the AC without having to log in to APs to perform any configuration. APs can then connect to the AC. This function facilitates the deployment of a large number of APs. **Figure 8-3** shows how zero touch configuration is implemented.

Figure 8-3 Implementation of zero touch configuration



1. After MP1 is powered on, it exchanges Mesh Peering Open and Mesh Peering Confirm frames with MP2 that has associated with the AC using information including the default Mesh ID and pre-shared key. MP1 establishes a temporary insecure mesh connection with MP2 and establishes a route to the MPP.
2. MP1 obtains an IP address and AC's IP address from the DHCP server through the mesh connection.
3. MP1 discovers and associates with the AC through the mesh connection and establishes a temporary CAPWAP tunnel to obtain the configuration from the AC.
4. After MP1 obtains the new configuration, it sends a Mesh Peering Close frame to tear down the temporary insecure mesh connection.
5. MP1 resets automatically and exchanges Mesh Peering Open and Mesh Peering Confirm frames with MP2 using the new mesh configuration for key negotiation. After MP1 and MP2 negotiate the key for communication, the two MPs establish a formal secure mesh link.

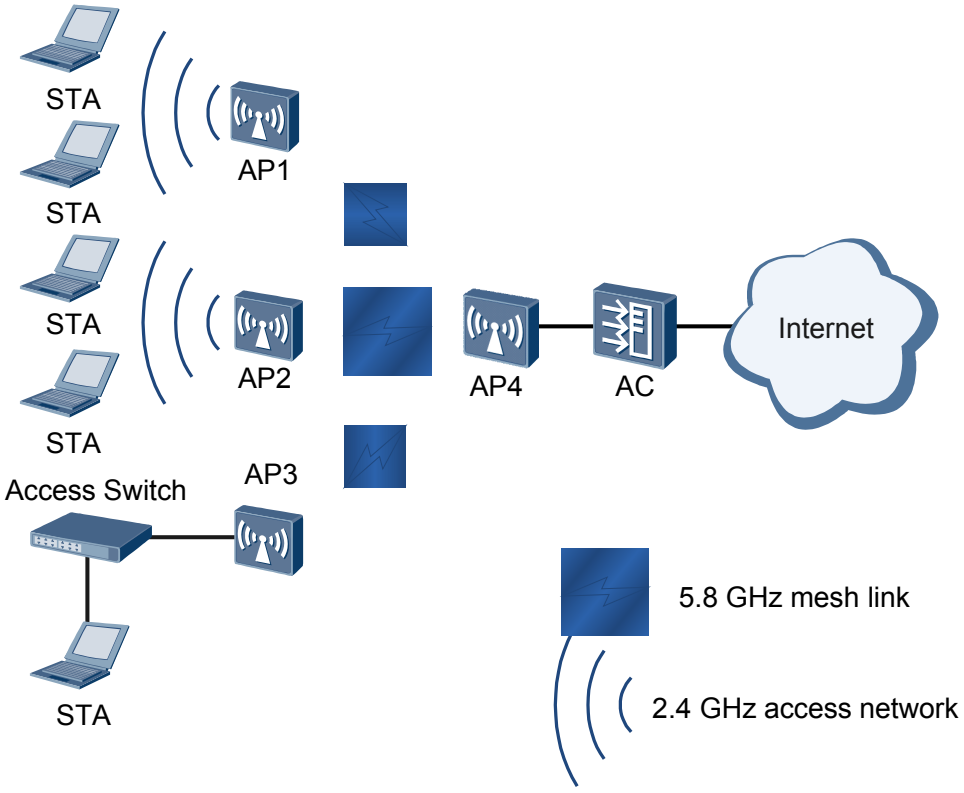
6. MP1 re-establishes a secure CAPWAP tunnel with the AC using the new configuration.
7. When MP1 cannot establish a mesh link with MP2 within a long period, the default configuration is restored, and the whole process starts from step 1 until MP1 establishes a secure CAPWAP tunnel with the AC using the new configuration.

8.3 Applications

Mesh Wireless Bridging

In **Figure 8-4**, AP1 to AP3 provide network access service for wired and wireless users. The three APs, however, cannot access the Internet in wired mode because of geographical or environmental restrictions. AP1 to AP3 can work with AP4 to build a WMN so that wireless users can connect to the Internet.

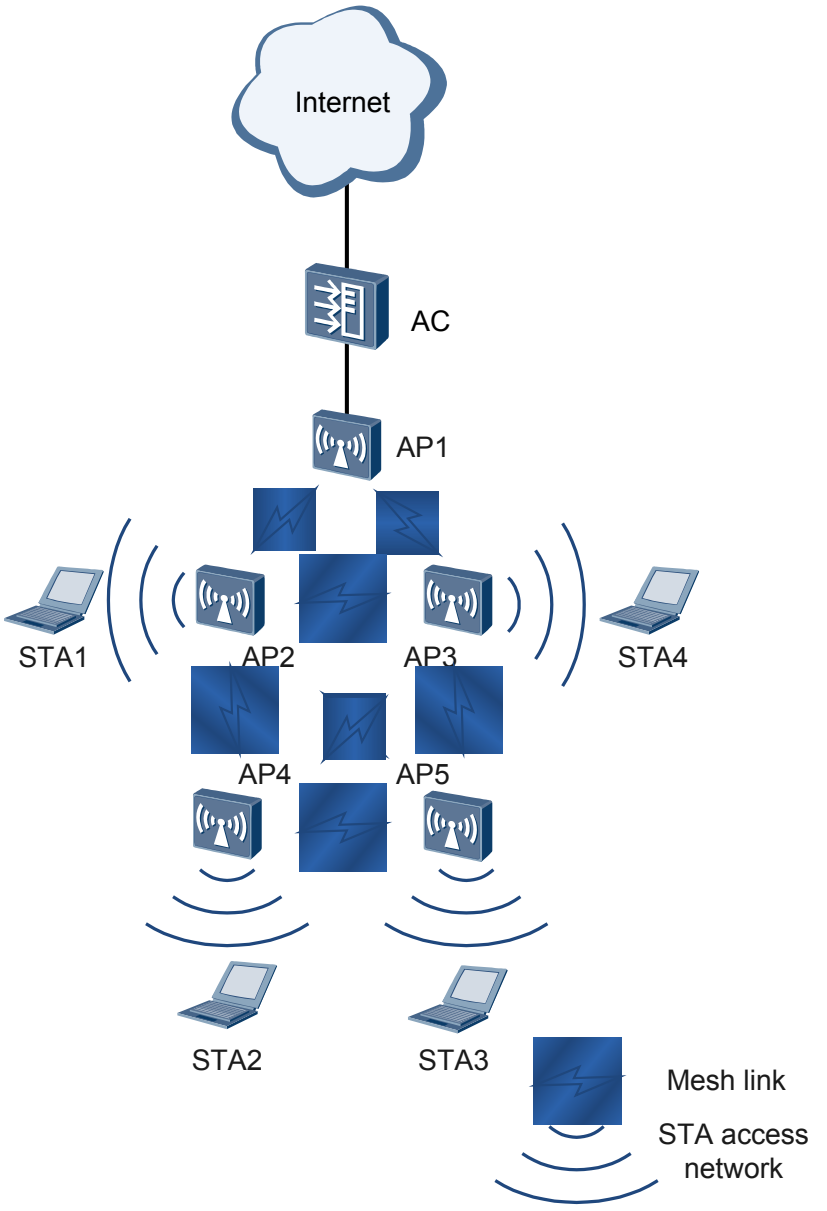
Figure 8-4 Mesh wireless bridging



WMN with One MPP

In **Figure 8-5**, AP2 to AP5 provide network access service for wireless users, and AP1 provides wired access to the Internet. AP1 to AP5 are fully meshed to establish a secure, auto-configured, and self-healing outdoor WMN, which facilitates fast and cost-effective WLAN deployment in outdoor environment where cabling is difficult.

Figure 8-5 WMN with one MPP



WMN with Multiple MPPs

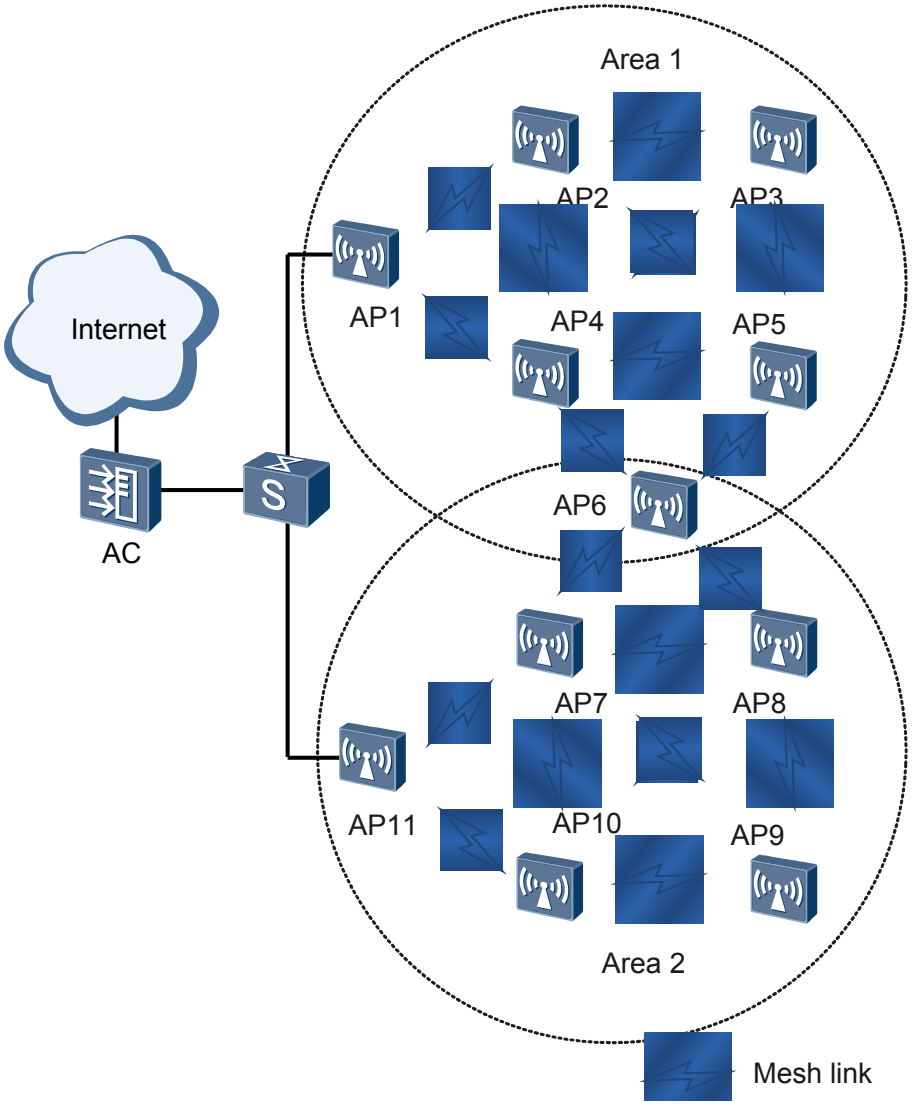
In **Figure 8-6**, AP1 and AP11 provide wired access to the Internet. AP2 to AP5 provide network access service for wired and wireless users in Area 1, and AP7 to AP10 provide network access service for wired and wireless users in Area 2. AP6 resides in the overlapping area between Area 1 and Area 2.

An MPP and MPs that establish mesh links with the MPP use the same wireless channels. If network access service needs to be provided for different areas, multiple MPPs need to work in different channels to prevent MPs from preempting wireless channels and improve coverage performance. Each MP can select the MPP with the minimum hops from the MP as the gateway to connect the wired network.

NOTE

If an AP connects to different MPPs through a WMN, for example, AP6 in **Figure 8-6** connects to two MPPs (AP1 and AP11), AP6 must support 2.4 GHz and 5 GHz frequency bands, while AP1 and AP11 must work in different frequency bands. An AP can connect to a maximum of two MPPs on a WMN.

Figure 8-6 WMN with multiple MPPs



8.4 References

The following table lists the references for this document.

Table 8-1 References

Document	Description
IEEE 802.11s	WLAN Mesh Standard

9 WLAN Positioning

About This Chapter

9.1 Introduction to Wireless Positioning

9.2 Principles

9.3 References

9.1 Introduction to Wireless Positioning

Definition

WLAN positioning involves WLAN tag positioning and terminal positioning.

WLAN tag positioning technology uses radio frequency identification (RFID) devices and a positioning system to locate a target through the WLAN. An AP sends the collected RFID tag information to a positioning server. The positioning server then computes the physical location and sends the location data to a third-party device so that users can view the location of a target through maps and tables.

Terminal positioning technology uses APs to collect strength information about radio signals in the surrounding environment to locate Wi-Fi terminals and rogue APs. The APs report the collected information to a positioning server. The positioning server computes locations of terminals based on AP's location and data received from the APs, and presents the computing results to users through a display terminal.

Purpose

Wireless positioning technology helps users efficiently implement network management and key asset control.

9.2 Principles

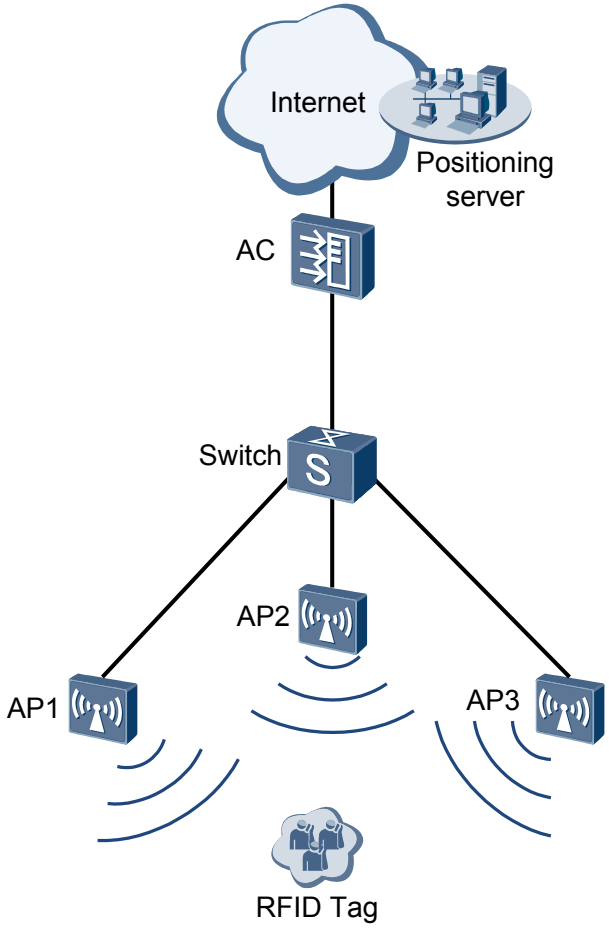
9.2.1 WLAN tag positioning

Concepts

As shown in **Figure 9-1**, the terminal positioning system includes at least three APs, one or more RFID tags, one or more ACs, a positioning server, and a location display terminal. Functions of each component are as follows:

- Radio frequency identification (RFID) tag: is manufactured by tag vendors to carry wireless location system data. For example, AeroScout manufactures RFID tags that are often placed or pasted to the objects to be located. The tag is a source device that needs to be located and can periodically send radio waves to surrounding devices.
- AP: receives location information sent by an RFID tag and forwards the information to the AC or directly sends it to a positioning server.
- AC: forwards the configuration instruction from the positioning server to APs. It can also forward location information received from an AP to the positioning server.
- Positioning server: computes the RFID tag location using a location algorithm (for example, three-point positioning) after receiving the location information and provides the computed data to user systems, including the system management software and image software.

Figure 9-1 Typical networking for the WLAN tag positioning system



Implementation

Figure 9-2 Working mechanism of the WLAN tag positioning system

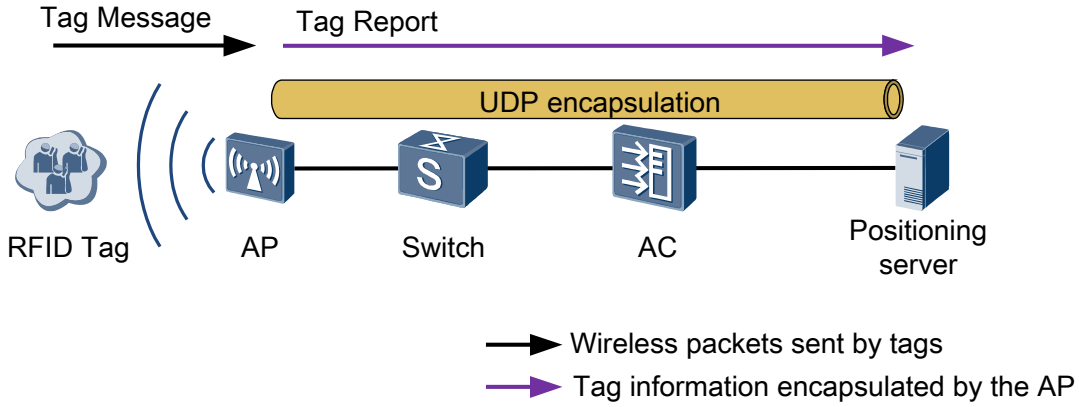


Figure 9-2 shows how wireless positioning is implemented.

1. The RFID tag sends a tag message.

   The RFID tag only sends 802.11 frames periodically to provide location information and does not need to connect to a WLAN.

   To enable more APs to receive tag messages, the RFID tag sends a tag message in all channels each time. A tag message usually contains location information required by a positioning server, and the frame format of the tag message varies depending on the vendor's tag device. A tag of AeroScout is used as an example here.

   - The **Address1** field indicates the destination address, which is a specified multicast address. The AP identifies an 802.11 packet as a tag message through the multicast address.
   - The **Address2** field indicates the source address, which is the MAC address of the RFID tag. According to this field, the wireless positioning system collects information about the same RFID tag that is received from different APs.
   - The **Address3** field indicates RFID tag information. The most important information in this field is about the channel that transmits the tag message. The AP determines whether the channel information in the received tag message matches its working channel.
   - The **Address4** field is available only when the tag message needs to be transmitted on a wireless distribution system (WDS) network. This field indicates the extended RFID tag information.

   For details about the 802.11 MAC frame format, see **1.2.2 802.11 Standards**.

2. The AP receives the tag message and forwards it to the positioning server.

   a. When receiving a tag message frame, the AP records the location information such as the received signal strength indicator (RSSI), timestamp, rate, and channel of the frame. The RSSI is the most important information because the positioning server uses it to determine the distance between a tag and an AP. To ensure that the RSSI is accurate, the AP must filter out the tag messages received from adjacent channels. For example, when working in channel 1, the AP may receive the frames sent from a tag in channel 2. The RSSI is low because the AP and tag are located in different channels. As a result, the positioning server mistakenly considers that the tag is far away from the AP.

   b. The AP encapsulates all location information obtained from tag message frames into a UDP packet (tag report) and sends the packet to the positioning server directly or through the AC.

      The required location information and report mode vary depending on the vendor's positioning server. For example, the Ekahau Positioning Server requires that the location information should contain content of the tag message frames and the AP should report tag message frames immediately when receiving them; the AeroScout Positioning Server does not need content of the tag message frames and allows the AP to periodically report collected location information.

      The destination IP address and port number of a tag report packet are configured on the AC. If the destination address is set to the IP address of the positioning server, the tag report packet is directly sent to the positioning server. If the destination address is set to the AC IP address, the tag report packet is sent to the AC and forwarded by the AC to the positioning server. This configuration is used when the AP cannot be directly connected to the positioning server.

   c. The positioning server computes the location information.

      To accurately determine the tag location, the positioning server must receive location information about a tag from at least three APs. After receiving the tag information,

the positioning server uses the built-in computing algorithm to compute the tag location according to information including the RSSI, SNR, radio mode, the imported map, and AP positions. Then, the positioning server sends the location information to the graphical interface of the third-party device for presentation.

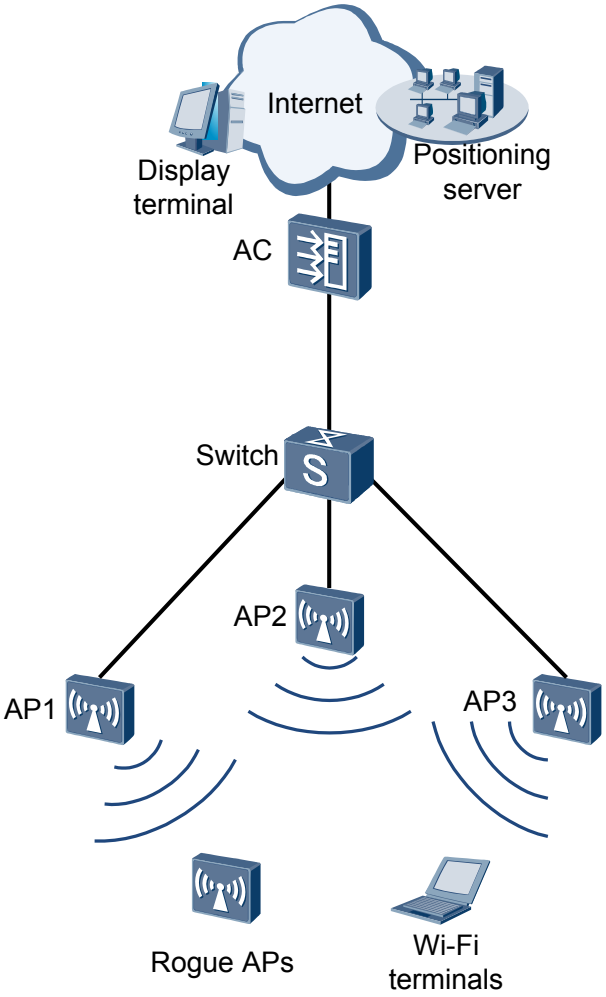
9.2.2 Terminal Positioning

Basic Concepts

As shown in **Figure 9-3**, the terminal positioning system includes at least three APs, one or more ACs, a positioning server, and a location display terminal. Functions of each component are as follows:

- AP: The APs collect wireless signals. The APs periodically switch channels to collect strength information about terminal signals in the surrounding environment on each channel and report the collected information to the positioning server.
- AC: The AC delivers terminal positioning configurations to the APs. In addition, the AC also classifies and filters the information received from the APs based on the device type (such as authorized terminals and rogue APs).
- Positioning server: The positioning server computes the signal transmission model according to locations of APs and obstacles, and calculates locations of terminals based on the information received from each AP. An NMS device is usually used as a positioning server.
- Display terminal: The display terminal draws maps and displays terminal locations on the map. The display terminal can be integrated to the positioning server.

Figure 9-3 Typical networking for the terminal positioning system



Implementation Principles

Terminal positioning technology locates terminals as follows:

1. APs collect strength information about radio signals and forwards the information to the positioning server.
   a. The APs periodically switch channels to collect frames sent from terminals in the surrounding environment on each channel and record frame information including RSSI information, timestamp, data rate, and channel information. RSSIs are essential in determining whether a terminal is near or far from the APs.
   b. The APs encapsulate the collected radio signal information into UDP packets and report the data to the positioning server in the following two modes:
      - APs report collected data to the AC. Then, the AC reports the data to the positioning server.

        When the network between the APs and positioning server is not reachable, the APs report data to the AC first. The AC then filters information about terminals and rogue APs before reporting the data to the positioning server.

- The APs directly report the collected data to the positioning server.

  If the network between the APs and positioning server is reachable, and the AC is not required to identify unauthorized APs, configure the APs to directly send data to the positioning server, which decreases CPU usage of the AC and reduces impacts of the positioning function on services.

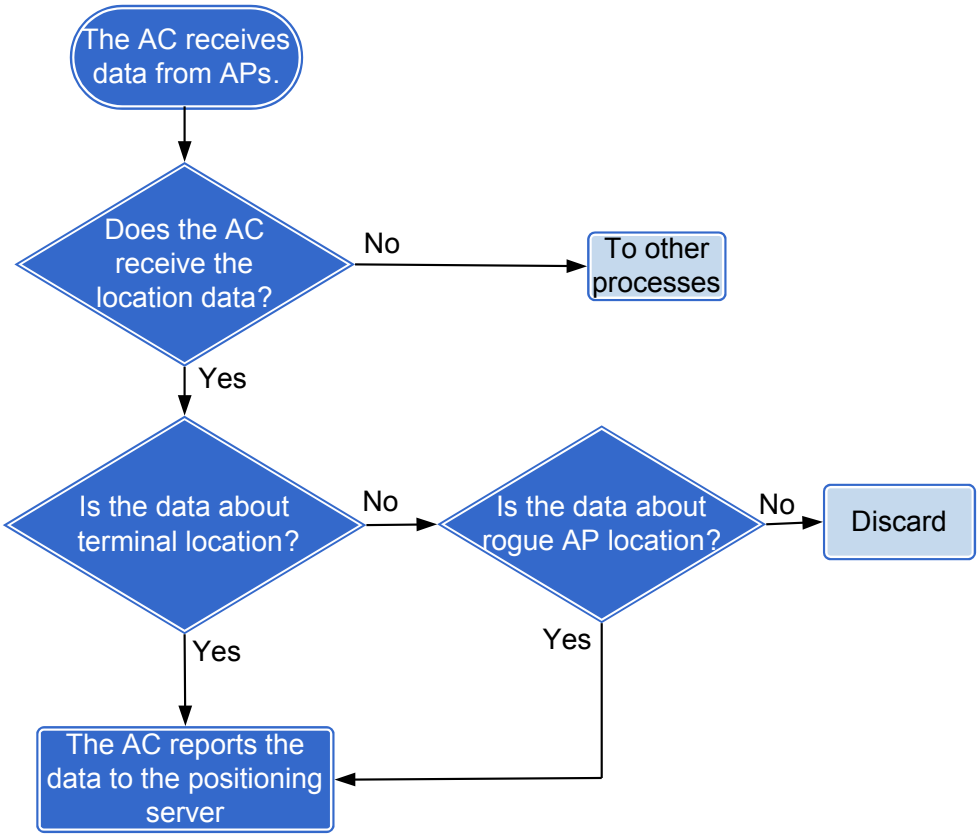
2. The AC reports the information received from APs to the positioning server.

   As shown in **Figure 9-4**, after receiving information from the APs, the AC processes the information as follows:

   a. Determine whether the data received from the APs is positioning data. If not, the data is processed in other ways.

   b. If the AC receives the location data, the AC processes the data in the following way: if the data is about terminal locations, the AC reports the data directly to the positioning server; if the data is about authorized AP locations, the AC discards the data; if the data is about rogue AP locations, the AC reports the data to the positioning server.

Figure 9-4 Processing positioning information



3. The positioning server computes the location information.

   The positioning process involves the offline phase and online phase.

   a. Offline phase: The positioning server divides the whole network into multiple equal area grids, computes the signal transmission model according to environment features (indoor/outdoor and obstacle features), calculates the theoretical differences among

RSSIs of a STA in the grid to all APs based on the imported AP location information, and stores the data into the database.

b. Online phase: At least three APs report terminal information to the positioning server after receiving the terminal information. The positioning server compares the information received from the APs with the information in the database to obtain the location of the terminal.

9.3 References

None